WRT-300BGN-R2

BLACK BOX NETWORK SERVICES

Pure Networking™ 802.11n 2T2R Wireless Router

Share a single xDSL/cable modem high-speed wireless Internet connection between up to 253 users.

Includes four wired LAN ports and one WAN port.
Transfer files at speeds up to 300 Mbps.

Customer Support Information

Order toll-free in the U.S.: Call 877-877-BBOX (outside U.S. call 724-746-5500)
FREE technical support 24 hours a day, 7 days a week: Call 724-746-5500 or fax 724-746-0746
Mailing address: Black Box Corporation, 1000 Park Drive, Lawrence, PA 15055-1018
Web site: www.blackbox.com • E-mail: info@blackbox.com

Trademarks Used in this Manual

Black Box and the Double Diamond logo are registered trademarks, and Pure Networking is a trademark, of BB Technologies, Inc.

Microsoft, Internet Explorer, Windows, and Windows Vista are registered trademarks of Microsoft Corporation.

Netscape and Navigator are registered trademarks of Netscape Communications Corporation.

Safari is a registered trademark of Apple, Inc.

Any other trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.

We're here to help! If you have any questions about your application
or our products, contact Black Box Tech Support at **724-746-5500**
or go to **blackbox.com** and click on "Talk to Black Box."
You'll be live with one of our technical experts in less than 30 seconds.

Federal Communications Commission and Industry Canada Radio Frequency Interference Statements

Class B Digital Device. This equipment has been tested and found to comply with the limits for a Class B computing device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. If this equipment does cause harmful interference to radio or telephone reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult an experienced radio/TV technician for help.

Caution:

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

To meet FCC requirements, shielded cables and power cords are required to connect this device to a personal computer or other Class B certified device.

This digital apparatus does not exceed the Class B limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de classe B prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

Instrucciones de Seguridad
(Normas Oficiales Mexicanas Electrical Safety Statement)

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc..
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.
12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.
13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.
14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.
15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.
16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.
17. Cuidado debe ser tomado de tal manera que objectos liquidos no sean derramados sobre la cubierta u orificios de ventilación.
18. Servicio por personal calificado deberá ser provisto cuando:
    - A: El cable de poder o el contacto ha sido dañado; u
    - B: Objectos han caído o líquido ha sido derramado dentro del aparato; o
    - C: El aparato ha sido expuesto a la lluvia; o
    - D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o
    - E: El aparato ha sido tirado o su cubierta ha sido dañada.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) as of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacturer must therefore be followed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not Intended for Use

None.

Table of Contents

1. Specifications 8
2. Overview 9
2.1 Introduction 9
2.2 Features 9
2.3 Safety Information 9
2.4 System Requirements 10
2.5 What's Included 10
2.6 Front Panel 10
2.7 Back Panel 11
3. System and Network Setup 12
3.1 Build the Network Connection 12
3.2 Connecting to the Router via a Web Browser 13
3.2.1 Windows 95/98/Me IP Address Setup 13
3.2.2 Windows 2000 IP Address Setup 14
3.2.3 Windows XP IP Address Setup 15
3.2.4 Windows Vista IP Address Setup 17
3.2.5 Router IP Address Lookup 19
3.3 Using Quick Setup 22
3.3.1 Setup Procedure for Cable Modem 24
3.3.2 Setup Procedure for Fixed IP xDSL 24
3.3.3 Setup Procedure for PPPoE xDSL 25
3.3.4 Setup Procedure for PPTP xDSL 26
3.3.5 Setup Procedure for L2TP xDSL 27
3.3.6 Setup Procedure for Telstra Big Pond 28
3.4 Basic Setup 30
3.4.1 Time Zone and Time Auto-Synchronization 30
3.4.2 Change Management Password 31
3.4.3 Remote Management 32
3.5 Setup Internet Connection (WAN Setup) 33
3.5.1 Setup Procedure for Dynamic IP 34
3.5.2 Setup Procedure for Static IP 35
3.5.3 Setup Procedure for PPPoE 36
3.5.4 Setup Procedure for PPTP 37
3.5.5 Setup Procedure for L2TP 38
3.5.6 Setup Procedure for Telstra Big Pond 39
3.5.7 Setup Procedure for DNS 39
3.5.8 Setup Procedure for DDNS 40
3.6 Wired LAN Configurations 42
3.6.1 LAN IP Section 42
3.6.2 DHCP Server 43
3.6.3 Static DHCP Leases Table 43

3.7 Wireless LAN Configurations 45
3.7.1 Basic Wireless Settings 46
3.7.2 Advanced Wireless Settings 52
3.7.3 Wireless Security 54
3.7.4 Wireless Access Control 57
3.7.5 Wi-Fi Protected Setup (WPS) 59
3.7.6 Security Tips for Wireless Networks 61
4. Advanced Functions 62
4.1 Quality of Service (QoS) 62
4.1.1 Basic QoS Settings 62
4.1.2 Add a New QoS Rule 64
4.2 Network Address Translation (NAT) 64
4.2.1 Basic NAT Settings (Enable or Disable NAT Function) 65
4.2.2 Port Forwarding 66
4.2.3 Virtual Server 67
4.2.4 Port Mapping for Special Applications 68
4.2.5 UPnP Setting 70
4.2.6 ALG Settings 71
4.3 Firewall 72
4.3.1 Access Control 73
4.3.2 URL Blocking 76
4.3.3 DoS Attack Prevention 78
4.3.4 Demilitarized Zone (DMZ) 80
4.4 System Status 82
4.4.1 System Information and Firmware Version 82
4.4.2 Internet Connection Status 83
4.4.3 Device Status 83
4.4.4 System Log 84
4.4.5 Security Log 84
4.4.6 Active DHCP Client List 85
4.4.7 Statistics 85
4.5 Configuration Backup and Restore 86
4.6 Firmware Upgrade 87
4.7 System Reset 88
Appendix A: Troubleshooting 89
A.1 Problems/Solutions 89
A.2 Calling Black Box 90
A.3 Shipping and Packaging 90
Appendix B: Glossary 91

1. Specifications

Antennas: (2) 3-dBi Pifa antennas (2T2R MIMO technology)

Certification: FCC, CE Flash: 4 MB

Data Rate: 11b: 1/2/5.5/11 Mbps;
11g: 6/9/12/24/36/48/54 Mbps;
11n (20 MHz): MCS0-7, up to 144 Mbps;
11n (40 MHz): MCS0-7, up to 300 Mbps

SDRAM: 16 MB

Transmit Power: 802.11n: 15 dBm±1 dBm;
802.11g: 15 dBm±1 dBm;
802.11b: 18 dBm±1 dBm

User Controls: (1) Radio ON/OFF switch; (1) Reset/WPS button

Interface: (1) RJ-45 WAN, (4) RJ-45 LAN

Connectors: LAN: (4) 10-/100-Mbps RJ-45 UTP;
WAN: (1) 10-/100-Mbps RJ-45 UTP

Indicators: (7) LEDs: (1) Power, (1) WLAN, (1) LAN, (4) Port (1–4)

Temperature: 32–104° F (0 –40° C)

Humidity: 10–90% (Noncondensing)

Power: 5-VDC, 1-A switching power adapter

Size: 1.2"H x 6.2"W x 5"D (3 x 15.7 x 12.7 cm)

Weight: 0.5 lb. (0.2 kg)

2. Overview

2.1 Introduction

With this Wireless Broadband Router, small office/home office (SOHO) users' computers and network devices can share a single xDSL/cable modem Internet connection at high speed. Easy install procedures enable computer users to set up a network environment within minutes. When you add computers and network-enabled devices, you can expand the number of network slots simply by attaching a hub or switch to extend the scope of your network.

With built-in IEEE 802.11b/g/n wireless network capability, all computers and wireless-enabled network devices (including PDAs, cellular phones, game consoles, and more!) can connect to this wireless router without additional cabling. New Draft-N wireless capability also gives you the highest speed for wireless. With a compatible wireless card installed in your PC, you can transfer files at up to 300 Mbps. Plus, the radio coverage area is doubled.

2.2 Features

- High Internet access throughput
- Enables multiple users to share a single Internet line
- Supports up to 253 users
- Share a single cable or xDSL Internet connection
- Access private LAN servers from the Internet
- Four wired LAN ports (10/100 Mbps) and one WAN port (10/100 Mbps)
- Provides IEEE 802.11b/g/n wireless LAN capability
- Supports DHCP (Server/Client) for easy IP address setup
- Supports multiple wireless modes such as: AP, Station Infrastructure, Wireless Bridge, and Universal Repeater
- Advanced network and security features include: Special Applications, QoS, DMZ, Virtual Servers, Access Control, and Firewall
- Allows you to monitor the router's status via: DHCP Client Log, System Log, Security Log, and Device/Connection Status
- Easy-to-use, Web-based GUI for network configuration and management purposes
- Remote management function allows configuration and upgrades from a remote computer (over the Internet)
- Auto MDI/MDI-X function for all wired Ethernet ports

2.3 Safety Information

For safety, follow these instructions:

1. This router is designed for indoor use only; DO NOT place this router outdoors.
2. DO NOT put this router at or near hot or humid places, such as a kitchen or bathroom, or leave it in the car in summer.
3. DO NOT pull any connected cable with force; disconnect it from the router first.
4. If you want to place this router in a high place or hang it on the wall, make sure the router is firmly secured. Falling from a high place would damage the router and its accessories, and void its warranty.
5. Router accessories, such as an antenna and power supply, are dangerous for small children under three years old since they contain small parts. KEEP THIS ROUTER OUT OF THE REACH OF CHILDREN!
6. The router will become hot when used for long time (this is normal and is not a malfunction). DO NOT put this router on paper, cloth, or other flammable materials.
7. There are no user-serviceable parts inside the router. If the router is not working properly, contact Black Box Technical Support at 724-746-5500. DO NOT disassemble the router; this will void the warranty.

8. If the router falls into water when it's powered, DO NOT pick it up. Switch the electrical power off before you do anything, or contact an experienced technician for help.
9. If you smell something strange or see smoke coming from the router or power supply, remove the power supply or switch the electrical power off immediately, and call Black Box Technical Support.

2.4 System Requirements

- Internet connection provided by xDSL or cable modem with a RJ-45 Ethernet port.
- Computer or network devices with wired or wireless network interface card.
- Web browser (Microsoft® Internet Explorer® 4.0 or above, Netscape® Navigator® 4.7 or above, Opera Web browser, or Safari® Web browser).
- An available AC power socket (100–240 VAC, 50/60 Hz)

2.5 What's Included

Your package should contain the following items. If anything is missing or damaged, contact Black Box Technical Support at 724-746-5500.

- Wireless router
- A/C power adapter
- This user's manual on CD-ROM

2.6 Front Panel

Figure 2-1 illustrates the router's front panel indicators. Table 2-1 describes the LEDs.

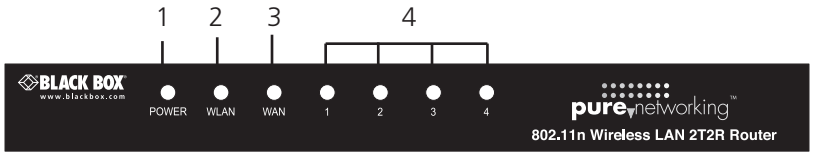


Figure 2-1. The router's front panel.

Table 2-1. Front panel components.

Number	LED Name	Light Status	Description
1	PWR	On	Router is switched on and correctly powered.
2	WLAN	On	Wireless WPS function is enabled.
		Flashing	Wireless LAN activity (transferring or receiving data).
		Off	Wireless network is switched off.
3	WAN LNK/ACT	On	WAN port is connected.
		Flashing	WAN activity (transferring or receiving data).
		Off	WAN port is not connected.
4	LNK/ACT (1–4)	On	The corresponding LAN port is connected.
		Off	The corresponding LAN port is not connected.
		Flashing	LAN activity (transferring or receiving data).

2.7 Back Panel

Figure 2-2 shows the router's back panel. Table 2-2 describes its components.

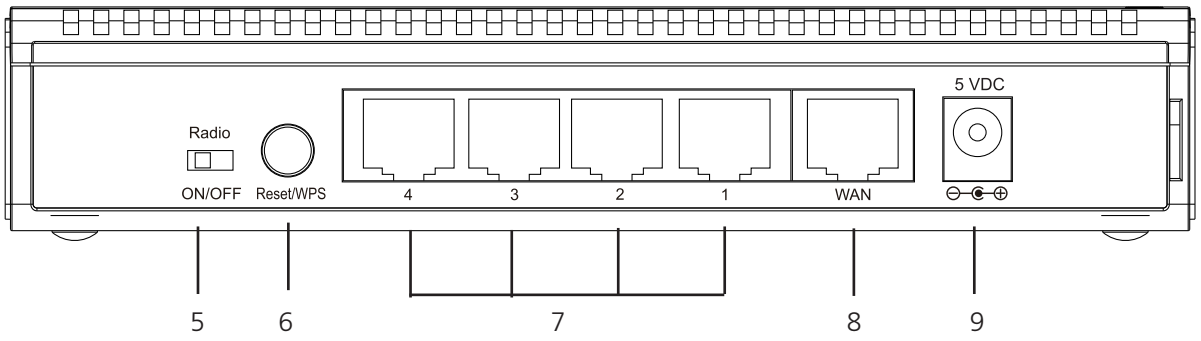


Figure 2-2. The router's back panel.

Table 2-2. Back panel components.

Number	Item Name	Description
5	Radio ON/OFF	Switch the button to activate or deactivate the wireless functions.
6	Reset/WPS	Reset the router to factory default settings (clear all settings) or start the WPS function. Press this button and hold it for 10 seconds to restore all settings to factory defaults, and press this button for less than 5 seconds to start the WPS function.
7	RJ-45 connectors	Local Area Network (LAN) ports 1 to 4.
8	WAN	Wide Area Network (WAN/Internet) port.
9	Power	Plug in your A/C power adapter to the 5-VDC power connector.
10	Not shown in diagram	(2) 3-dBi Pifa antennas (2T2R MIMO technology internal antennas)

3. System and Network Setup

3.1 Build the Network Connection

Follow these instructions to build the network connection between your new wireless router and your computers and network devices:

1. Using Ethernet cable, connect your xDSL/cable modem to the router's WAN port. See Figure 3-1.

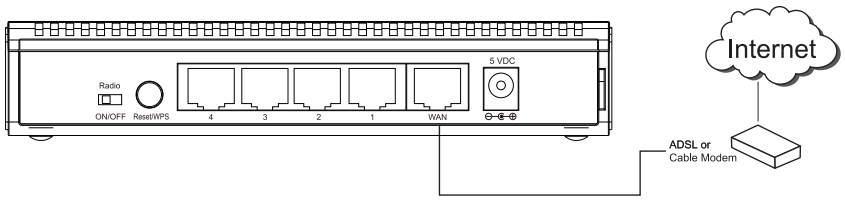


Figure 3-1. xDSL cable/modem connection.

2. Connect all your computers, network devices (network-enabled consumer devices other than computers, such as game consoles, or switches/hubs) to the router's LAN ports. See Figure 3-2.

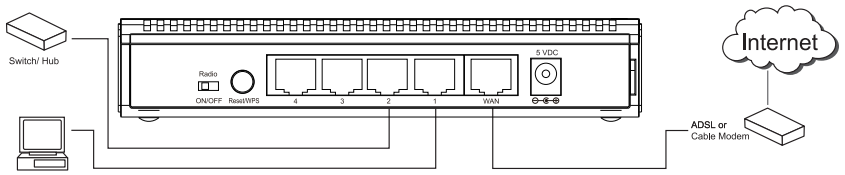


Figure 3-2. Connect devices to LAN ports.

3. Connect the A/C power adapter to the wall socket, and then connect it to the router's power socket. See Figure 3-3.

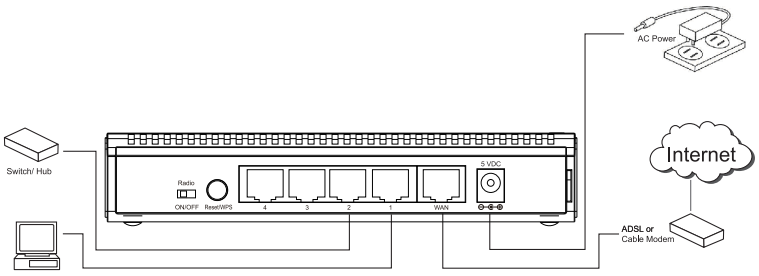


Figure 3-3. Connect the power.

4. Check all front-panel LEDs. The PWR LED should be steadily on, and the WAN and LAN LEDs should be on if the computer/network device connected to the respective port of the router is powered on and correctly connected. If the PWR LED is not on or any LED you expected to be on is not, recheck the cabling or go to Appendix A, Troubleshooting.

3.2 Connecting to the Router via a Web Browser

After you build the network connection, the next step is setting up the router with proper network parameters so it can work properly in your network environment.

Before you can connect to the router and start configuration procedures, your computer must be able to get an IP address automatically (use dynamic IP address). If it's set to use a static IP address or you're unsure, see the following instructions to configure your computer to use a dynamic IP address:

If the operating system of your computer is:

- Windows® 95/98/Me: go to Section 3.2.1
- Windows 2000: go to Section 3.2.2
- Windows XP: go to Section 3.2.3
- Windows Vista®: go to Section 3.2.4

3.2.1 Windows 95/98/Me IP Address Setup

1. Click on the Start button (it should be located at the lower-left corner of your computer), then click on control panel. Double-click the "Network" icon, and the Network window will appear. Select "TCP/IP," then click on "Properties." See Figure 3-4.

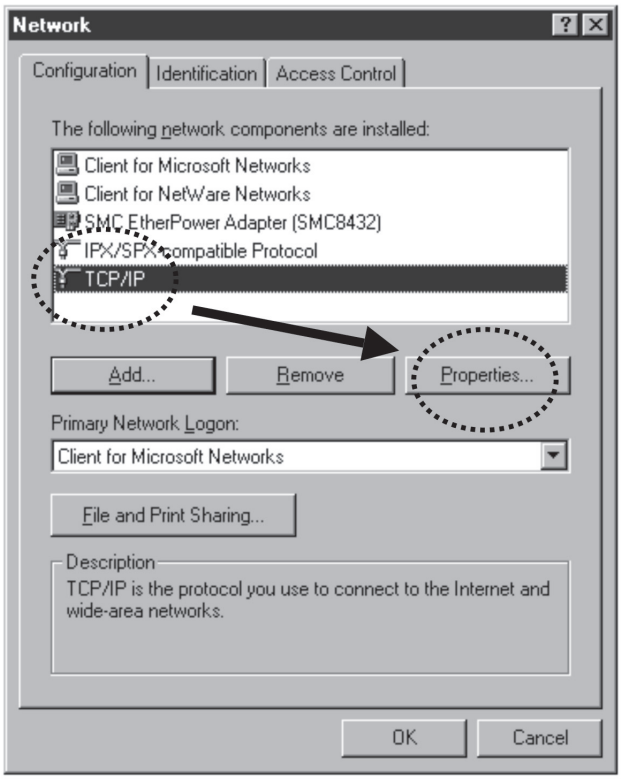


Figure 3-4. Network screen.

2. Select "Obtain an IP address from a DHCP server" and then click "OK." See Figure 3-5.

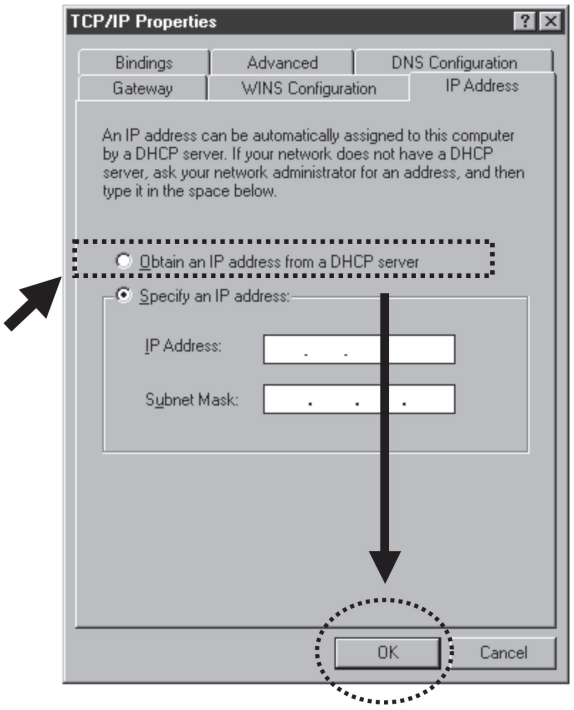

TCP/IP Properties
Bindings
Advanced
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address from a DHCP server
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

Figure 3-5. TCP/IP properties screen.

3.2.2 Windows 2000 IP Address Setup

1. Click on the "Start" button (it should be located at the lower-left corner of your computer), then click on the control panel. Double-click "Network" and the "Dial-up Connections" icon; click "Local Area Connection," and the Local Area Connection Properties window will appear. Select "Internet Protocol (TCP/IP)" and then click on "Properties."

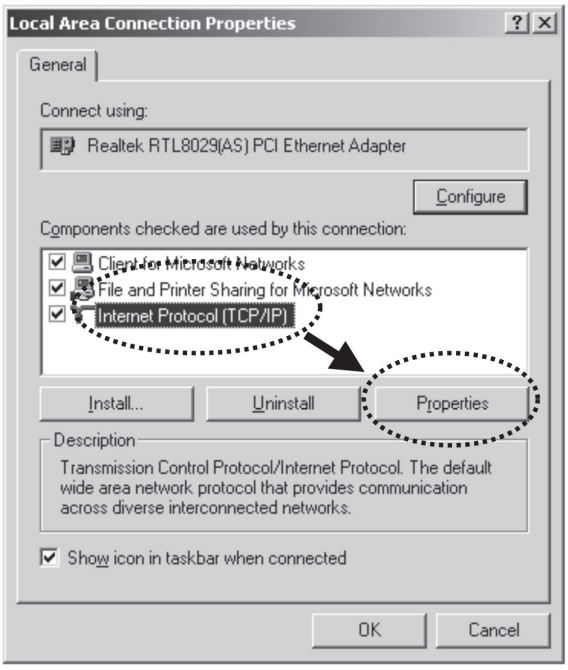


Figure 3-6. Select TCP/IP protocol.

2. Select "Obtain an IP address automatically "and "Obtain DNS server address automatically," then click "OK."

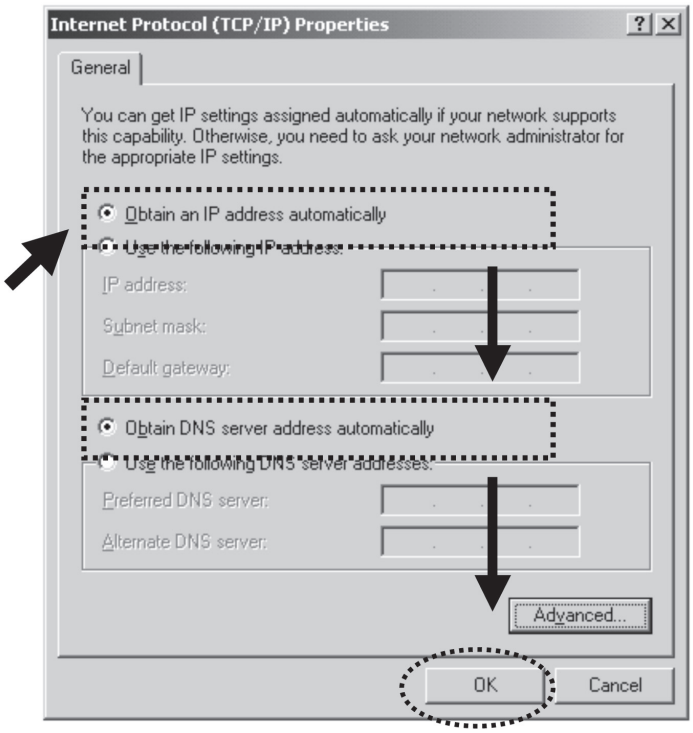

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 3-7. Obtain IP and DNS server addresses.

3.2.3 Windows XP IP Address Setup

1. Click on the "Start" button (it should be located at the lower-left corner of your computer), then on the control panel. Double-click "Network" and the "Internet Connections" icon, click "Network Connections," then double-click "Local Area Connection." The Local Area Connection Properties window will appear, and then click "Properties."

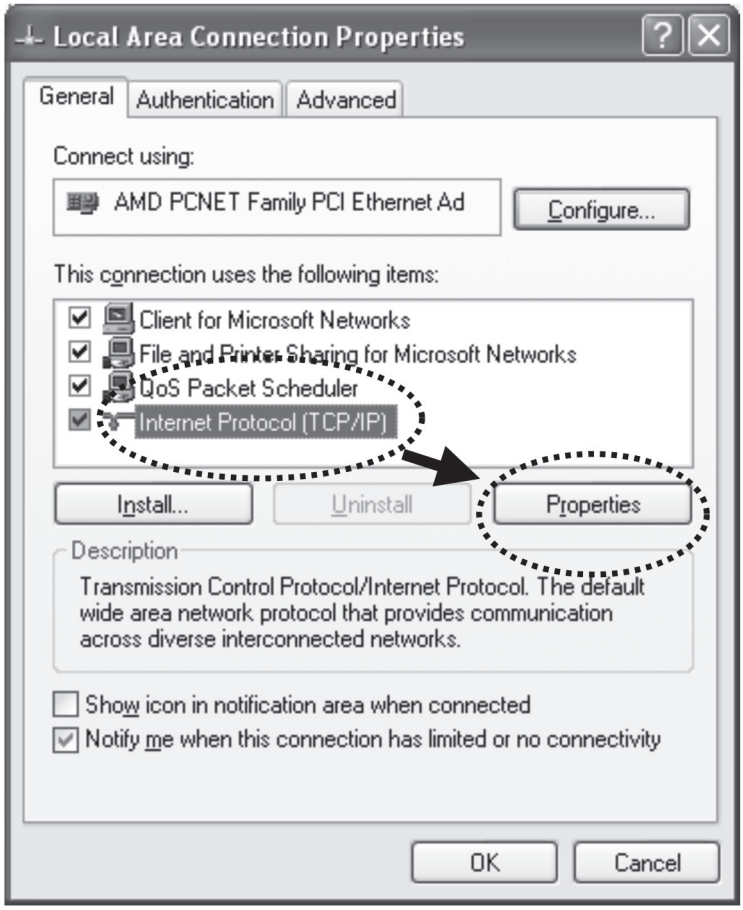
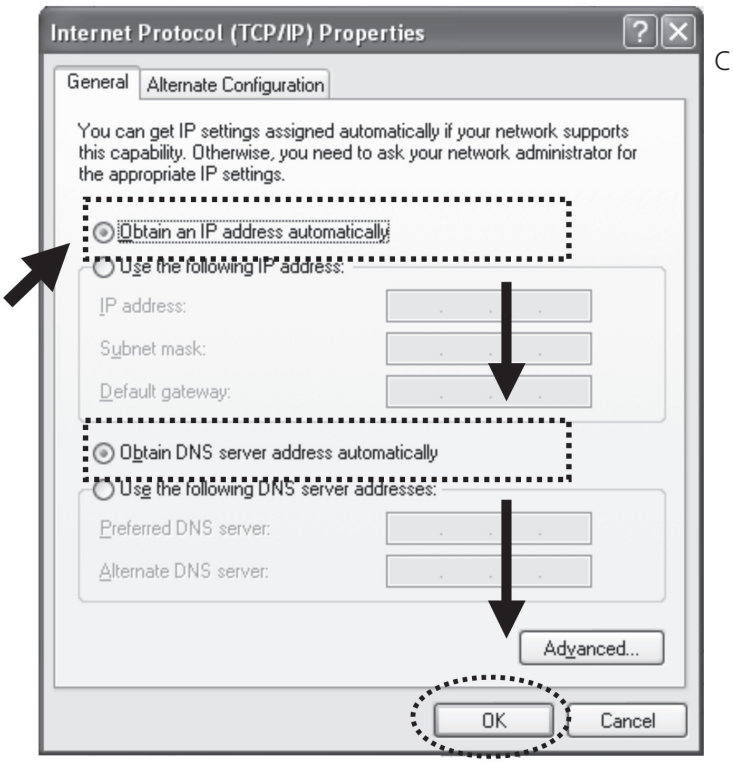


Figure 3-8. TCP/IP screen.

2. Select "Obtain an IP address automatically" and "Obtain DNS server address automatically," then click "OK."


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

C

Figure 3-9. Obtain DNS server address.

3.2.4 Windows Vista IP Address Setup

1. Click on the "Start" button (it should be located at the lower-left corner of your computer), then click on the control panel. Click "View Network Status and Tasks," and then click "Manage Network Connections." Right-click "Local Area Network," then select "Properties." The Local Area Connection Properties window will appear: select "Internet Protocol Version 4 (TCP / IPv4)," and then click "Properties."

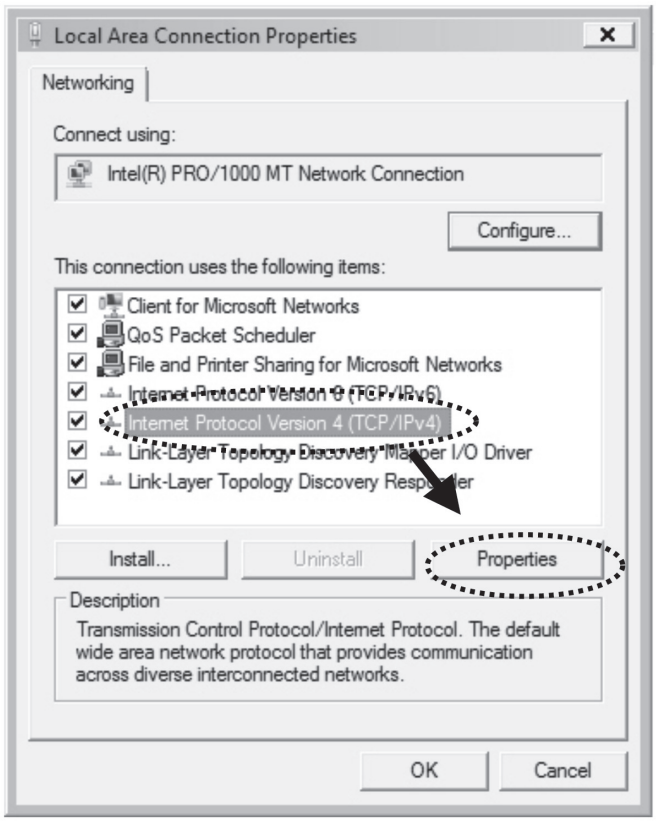


Figure 3-10. TCP/IP properties.

2. Select "Obtain an IP address automatically" and "Obtain DNS server address automatically," then click "OK."

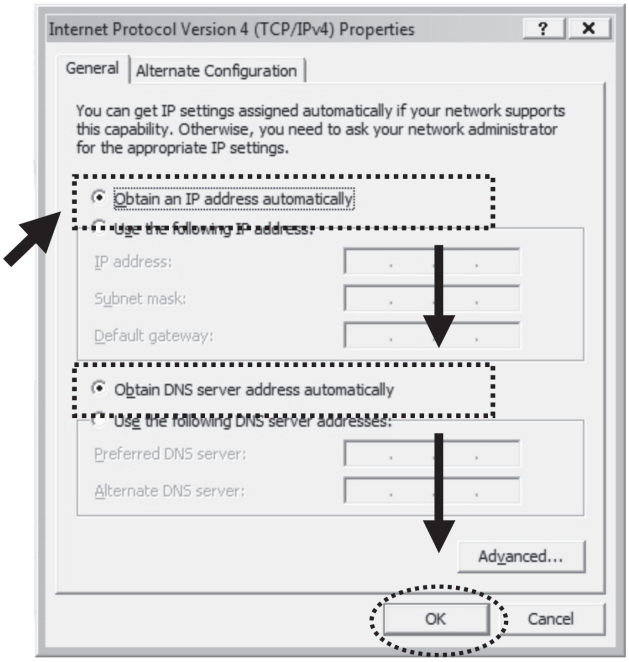

Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 3-11. Obtain IP and DNS addresses.

3.2.5 Router IP Address Lookup

After the IP address setup is complete, please click on "Start" at the bottom-lower corner of your desktop, then click "Run."

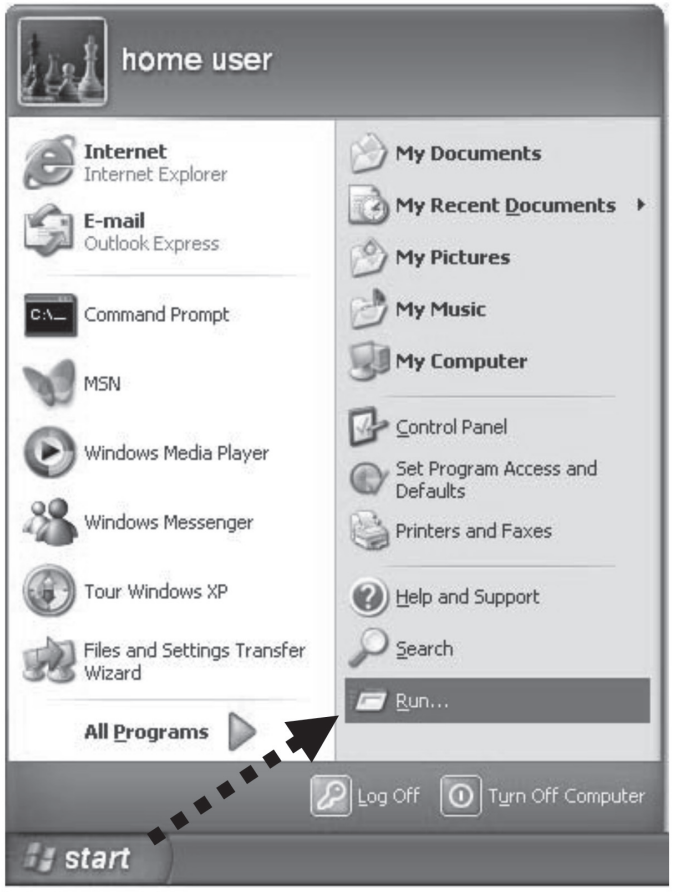


Figure 3-12. Click on the "Run" button.

Type cmd, then click "OK."

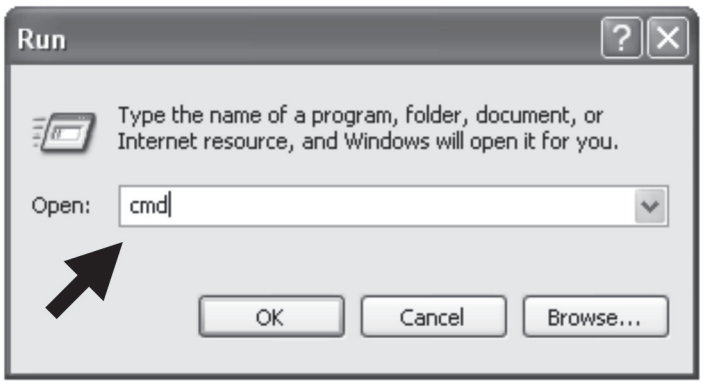


Figure 3-13. Run dialog box.

Type ipconfig, then press the "Enter" key. Check the IP address (which follows Default Gateway). (In this example, the IP address of the router is 192.168.2.1. Note that this value may be different.)

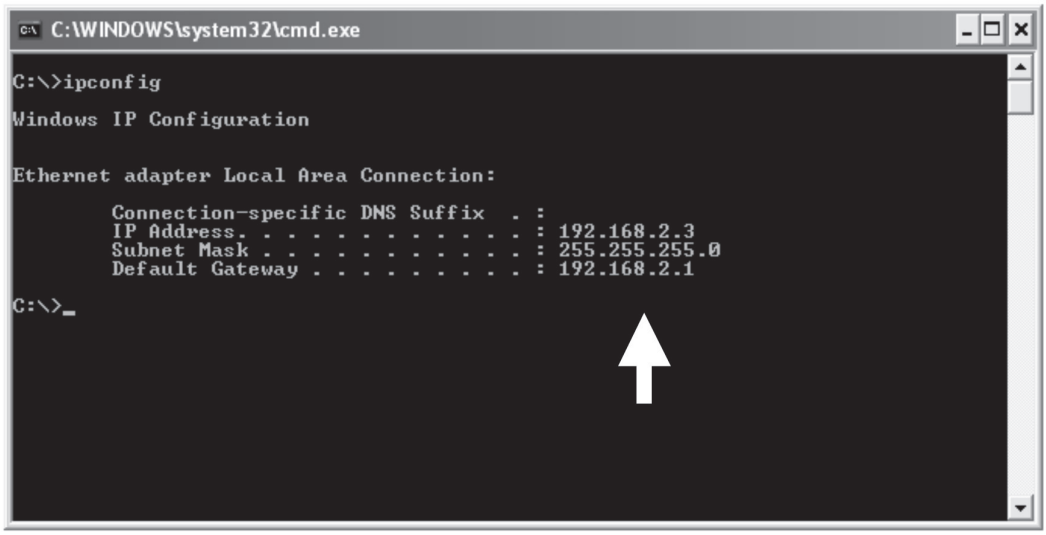

C:\WINDOWS\system32\cmd.exe
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.2.3
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.2.1
C:\>

Figure 3-14. Windows IP configuration.

NOTE: If the IP address of the gateway is not displayed or the address following IP Address begins with 169, re-check the network connection between your computer and router, and/or re-check every step of the network setup procedure.

3. Via a Web browser, connect the router's management interface by following the instructions below.

After your computer obtains an IP address from the router, start your Web browser, and type the router's IP address in the address bar. The following message should be shown (see Figure 3-15):

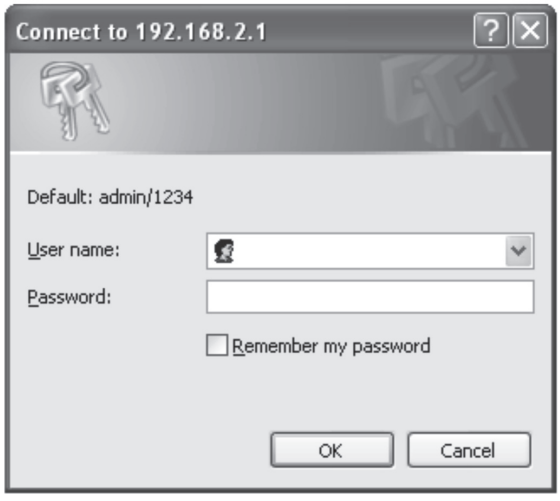


Figure 3-15. Connect screen.

Type the user name and the password. The default user name is "admin," and default password is "1234." Press the "OK" button, and the router's management interface screen appears (see Figure 3-16).

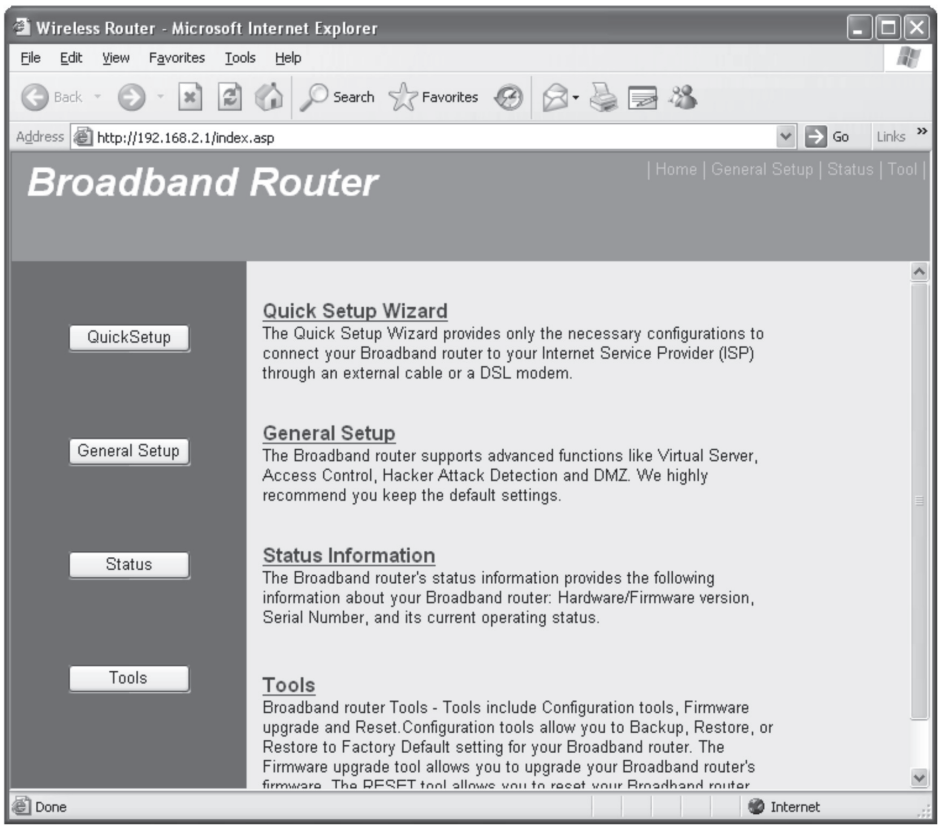

Wireless Router - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.2.1/index.asp
Go Links
Broadband Router
| Home | General Setup | Status | Tool |
QuickSetup
General Setup
Status
Tools
Quick Setup Wizard
The Quick Setup Wizard provides only the necessary configurations to connect your Broadband router to your Internet Service Provider (ISP) through an external cable or a DSL modem.
General Setup
The Broadband router supports advanced functions like Virtual Server, Access Control, Hacker Attack Detection and DMZ. We highly recommend you keep the default settings.
Status Information
The Broadband router's status information provides the following information about your Broadband router: Hardware/Firmware version, Serial Number, and its current operating status.
Tools
Broadband router Tools - Tools include Configuration tools, Firmware upgrade and Reset.Configuration tools allow you to Backup, Restore, or Restore to Factory Default setting for your Broadband router. The Firmware upgrade tool allows you to upgrade your Broadband router's
Done
Internet

Figure 3-16. Web management screen.

NOTE: If you can't see the Web management interface, and you're prompted to type the user name and password again, you may have typed the user name and password incorrectly. Retype the username and password again. If you're certain that the user name and password you typed are correct, go to Appendix A, Troubleshooting, and reset the default settings.

TIP: This page shows the four major setting categories: Quick Setup, General Setup, Status, and Tools. You can find the shortcut that leads to these categories at the upper right corner of every page. To jump to another category, simply click on the link.

3.3 Using Quick Setup

This router provides a Quick Setup procedure, which will help you to complete all required settings you need to access the Internet in a very short time. Follow the instructions in this section to complete the Quick Setup.

To go to the QuickSetup menu, click on the "Quick Setup" button.

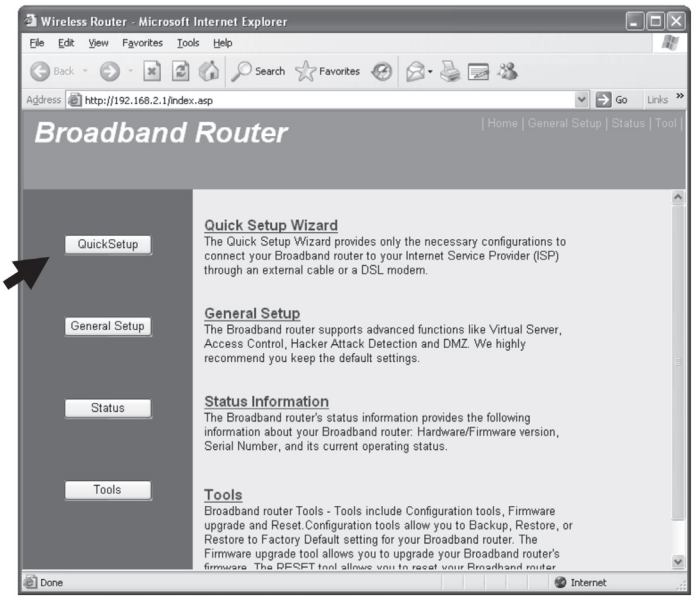

Wireless Router - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://192.168.2.1/index.asp
Broadband Router
Home | General Setup | Status | Tool
QuickSetup
General Setup
Status
Tools
Quick Setup Wizard
The Quick Setup Wizard provides only the necessary configurations to connect your Broadband router to your Internet Service Provider (ISP) through an external cable or a DSL modem.
General Setup
The Broadband router supports advanced functions like Virtual Server, Access Control, Hacker Attack Detection and DMZ. We highly recommend you keep the default settings.
Status Information
The Broadband router's status information provides the following information about your Broadband router: Hardware/Firmware version, Serial Number, and its current operating status.
Tools
Broadband router Tools - Tools include Configuration tools, Firmware upgrade and Reset.Configuration tools allow you to Backup, Restore, or Restore to Factory Default setting for your Broadband router. The Firmware upgrade tool allows you to upgrade your Broadband router's
Done
Internet

Figure 3-17. Quick Setup screen.

The following message will be displayed:

1. Set Time Zone

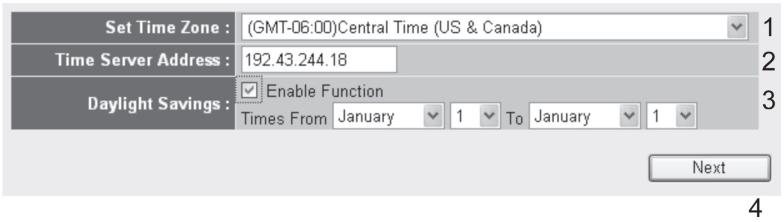


Figure 3-18. Set Time Zone screen.

Table 3-1. Time settings.

Item	Description
Set Time Zone (1):	Please press the down button, and a drop-down list will be shown. Choose the time zone of the location where you live.
Time Server Address (2):	Input the server's IP address/host name here.
Daylight Savings(3):	If the country where you live uses daylight savings time, check the "Enable Function" box, and choose the duration of daylight saving.

After you finish with the settings, click on the "Apply" (#4 in Figure 3-18) button.

NOTE: Several time servers are available on the Internet:
129.6.15.28 (time-a.nist.gov)
132.163.4.101 (time-a.timefreq.bldrdoc.gov)
131.107.1.10 (time-nw.nist.gov)

2. Broadband Type

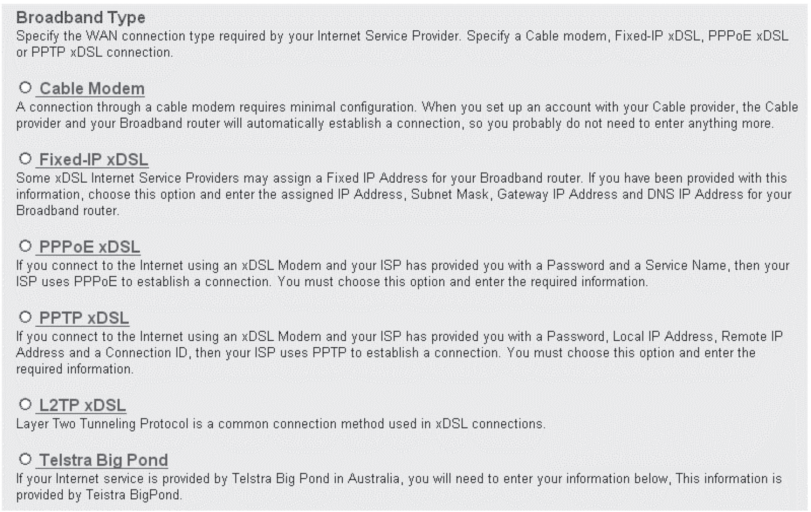

Broadband Type
Specify the WAN connection type required by your Internet Service Provider. Specify a Cable modem, Fixed-IP xDSL, PPPoE xDSL or PPTP xDSL connection.
Cable Modem
A connection through a cable modem requires minimal configuration. When you set up an account with your Cable provider, the Cable provider and your Broadband router will automatically establish a connection, so you probably do not need to enter anything more.
Fixed-IP xDSL
Some xDSL Internet Service Providers may assign a Fixed IP Address for your Broadband router. If you have been provided with this information, choose this option and enter the assigned IP Address, Subnet Mask, Gateway IP Address and DNS IP Address for your Broadband router.
PPPoE xDSL
If you connect to the Internet using an xDSL Modem and your ISP has provided you with a Password and a Service Name, then your ISP uses PPPoE to establish a connection. You must choose this option and enter the required information.
PPTP xDSL
If you connect to the Internet using an xDSL Modem and your ISP has provided you with a Password, Local IP Address, Remote IP Address and a Connection ID, then your ISP uses PPTP to establish a connection. You must choose this option and enter the required information.
L2TP xDSL
Layer Two Tunneling Protocol is a common connection method used in xDSL connections.
Telstra Big Pond
If your Internet service is provided by Telstra Big Pond in Australia, you will need to enter your information below, This information is provided by Teistra BigPond.

Figure 3-19. Broadband type screen.

Choose the broadband (Internet connection) type you're using on this page. There are six types of Internet connections, including:

- Cable Modem: go to Section 3.3.1
- Fixed-IP xDSL: go to Section 3.3.2
- PPPoE xDSL: go to Section 3.3.3
- PPTP xDSL: go to Section 3.3.4
- L2TP xDSL: go to Section 3.3.5.
- Telstra Big Pond: go to Section 3.3.6

If you're not sure, contact your Internet service provider. An incorrect Internet connection type will prevent you from connecting to the Internet.

If you want to go back to the previous step, press the "Back" button on the bottom of the Broadband Type page.

NOTE: Some service providers use Dynamic Host Configuration Protocol (DHCP) to assign IP addresses. In this case, choose "cable modem" as the Internet connection type, even if you're using another connection type, such as xDSL. Some cable modems use PPPoE; choose PPPoE xDSL even if you're using a cable modem.

3.3.1 Setup Procedure for Cable Modem

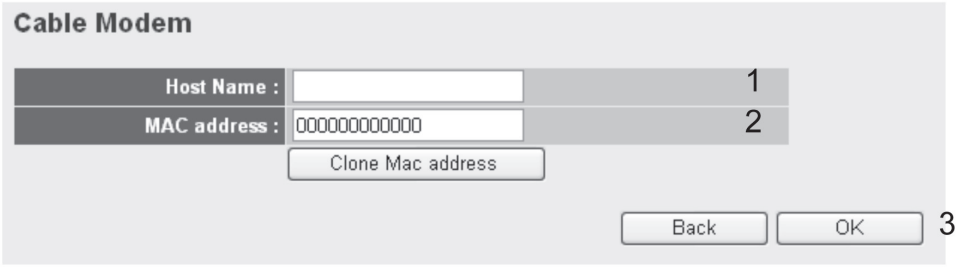


Figure 3-20. Cable modem setup screen.

Table 3-2. Cable modem setup options.

Item	Description
Host Name (1):	Input your computer's host name. This is optional and only required if your service provider asks you to do so.
MAC address (2):	Input your computer's MAC address here if your service provider only permits computers with certain MAC address to access the Internet. If you're using the computer that's used to connect to the Internet via a cable modem, simply press the "Clone MAC address" button to fill the MAC address field with your computer's MAC address.

After you finish with all settings, click on the "OK" (#3 in Figure 3-20) button; if you want to go back to the previous menu, click on the "Back" button.

3.3.2 Setup Procedure for Fixed-IP xDSL

NOTE: You can choose this Internet connection method if your service provider assigns a fixed IP address (also known as static address) to you, and you are not using DHCP or PPPoE protocol. Contact your service provider for more information.

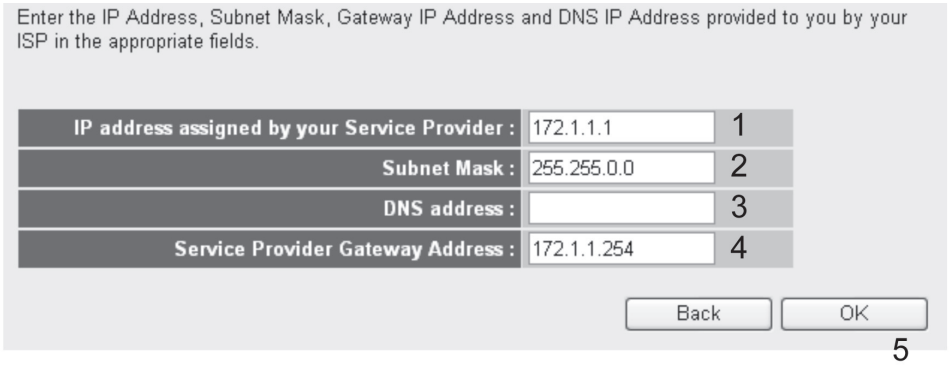


Figure 3-21. Fixed-IP xDSL setup.

Table 3-3. Fixed-IP xDSL options.

Item	Description
IP address assigned by your Service Provider (1):	Type in the IP address assigned by your service provider.
Subnet Mask (2):	Type in the subnet mask assigned by your service provider.
DNS address (3):	Type in the IP address of the DNS server provided by your service provider.
Service Provider Gateway Address (4):	Type in the IP address of the service provider gateway provided by your service provider.

NOTE: You must use the addresses provided by your Internet service provider; the wrong setting will cause connection problems.

When you finish with the settings, press the "OK" (5) button; if you want to go back to the previous menu, click on the "Back" button.

3.3.3 Setup Procedure for PPPoE xDSL

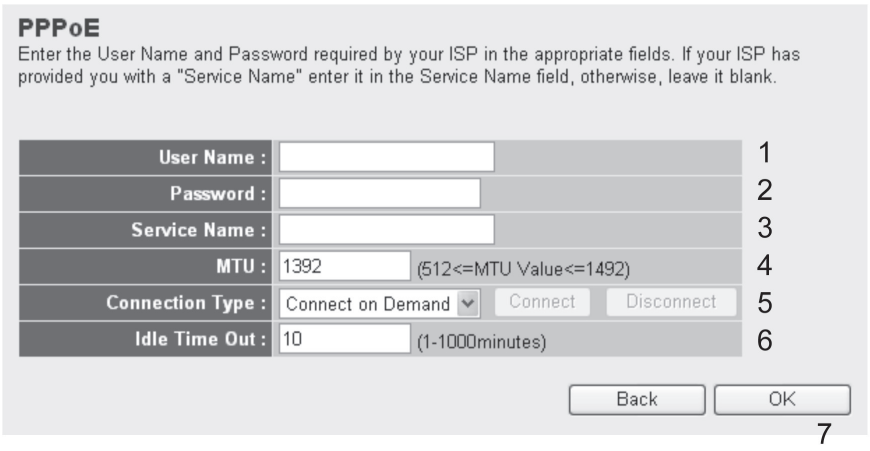


Figure 3-22. PPPoE setup screen.

Table 3-4. PPPoE setup options.

Item	Description
User Name (1):	Type in the user name assigned by your Internet service provider here.
Password (2):	Type in the password assigned by your Internet service provider here.
Service Name (3):	Give a name to this Internet service if you want; this is optional.
MTU (4):	Type in the MTU value of your network connection here. If you don't know, you can use the default value.
Connection Type (5):	Select the type of Internet connection you want to use (a detailed explanation is listed below).
Idle Time Out (6):	Type in idle time out (detailed explanation listed below).

When you finish with the settings, click on the "OK" (7) button; if you want to go back to the previous menu, click on the "Back" button.

MTU—Please use a default value if you don't know what it is or ask your service provider for a proper value.

Connection type—Choose from these options: continuous (keep Internet connection alive); do not disconnect; connect on demand (only connects to the Internet when there is a connection attempt); and manual (only connects to the Internet when you press the "Connect" button and disconnects when you press the "Disconnect" button).

Idle time out—Specify the time to shut down Internet connect after no activity is detected by minute. This option is only available when the connection type is "Connect on Demand."

3.3.4 Setup Procedure for PPTP xDSL

PPTP xDSL requires two kinds of settings: WAN interface setting (setup IP address) and PPTP setting (PPTP user name and password).

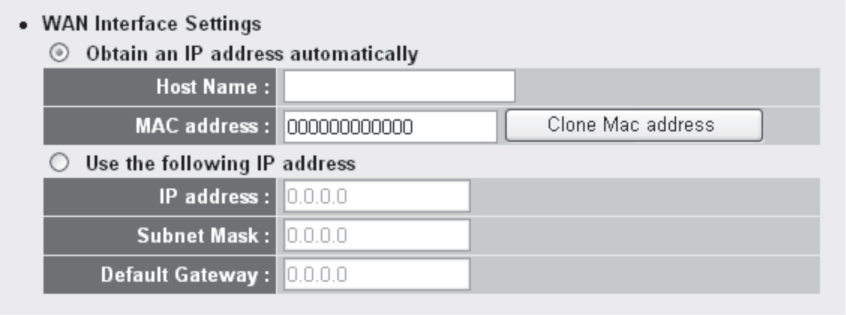


Figure 3-23. WAN interface settings screen.

Starting from the WAN interface setting, select how you obtain an IP address from your service provider here. Choose "Obtain an IP address automatically" (equal to DHCP, refer to the Cable Modem section in 3.3.1), or use the following IP address (that is, static IP address). WAN interface settings must be correctly set, or the Internet connection will fail even if the PPTP settings are correct. Contact your Internet service provider if you don't know what you should enter in these fields.

Now go to the PPTP settings section:

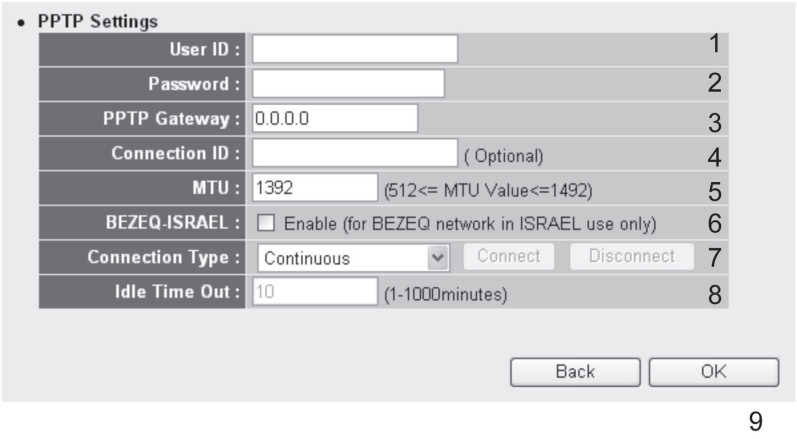


Figure 3-24. PPTP settings screen.

Table 3-5. PPTP settings options.

Item	Description
User ID (1):	Type in the user ID (user name) assigned by your Internet service provider here.
Password (2):	Type in the password assigned by your Internet service provider here.
PPTP Gateway (3):	Type in the IP address of PPTP gateway assigned by your Internet service provider here.

Table 3-5 (continued). PPTP settings options.

Item	Description
Connection ID (4):	Type in the connection ID here; this is optional and you can leave it blank.
MTU (5):	Type in the MTU value of your network connection here. If you don't know it, you can use the default value.
BEZEQ-ISRAEL (6):	Setting item BEZEQ-ISRAEL is only required to be checked if you're using the service provided by BEZEQ network in Israel.
Connection type (7):	Select the type of Internet connection you want to use. Refer to the previous section for detailed descriptions.
Idle Time Out (8):	Type in the idle time out for the Internet connection you want to use. Refer to the Section 3.3.3 for detailed descriptions.

When you finish with all settings, click on the "OK" (9) button; if you want to go back to the previous menu, click on the "Back" button.

3.3.5 Setup Procedure for L2TP xDSL

L2TP is another popular connection method for xDSL and other Internet connection types, and all required setting items are the same as the PPTP connection.

Like PPTP, there are two kinds of required settings, starting with WAN Interface Settings.

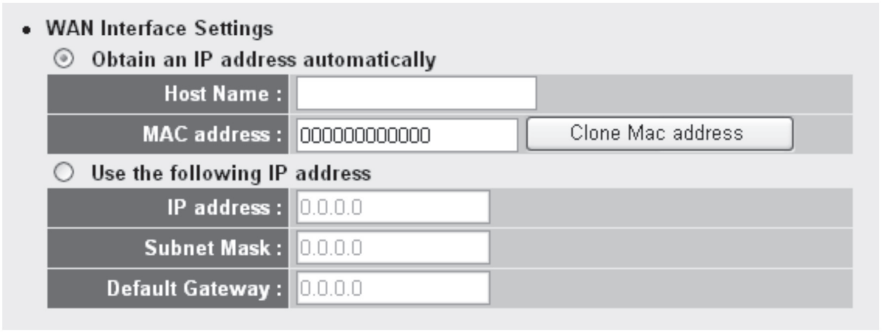


Figure 3-25. WAN interface settings.

Select how you obtain an IP address from your service provider here. Choose "Obtain an IP address automatically" (equal to DHCP—refer to Section 3.2.1), or "Use the following IP address" (equal to static IP address—refer to Section 3.5.2).

WAN interface settings must be correctly set, or the Internet connection will fail even if the PPTP settings settings are correct. Contact your Internet service provider if you don't know how you should fill in these fields.

Next, go to the L2TP settings section.

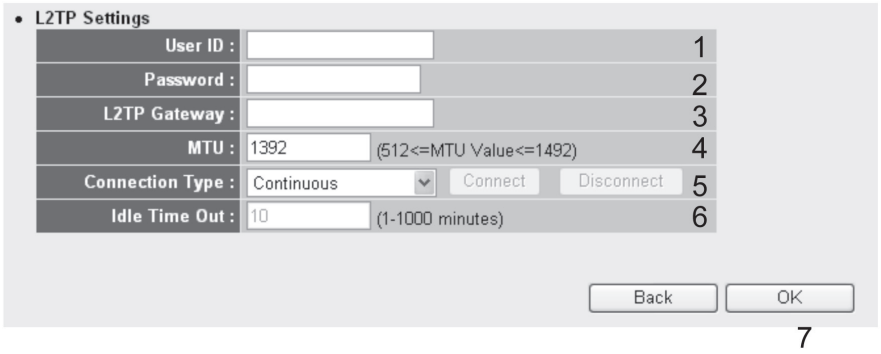


Figure 3-26. L2TP settings screen.

Table 3-6. L2TP options.

Item	Description
User ID (1):	Type in the user ID (user name) assigned by your Internet service provider here.
Password (2):	Type in the password assigned by your Internet service provider here.
L2TP Gateway (3):	Type in the PPTP gateway's IP address assigned by your Internet service provider here.
MTU (4):	Type in the network connection's MTU value here. If you don't know, you can use the default value.
Connection type (5):	Select the type of Internet connection you want to use; refer to the last section for detailed descriptions.
Idle Time Out (6):	Type in the idle time out of the Internet connection you want to use, and refer to the last section for detailed descriptions.

When you finish with all settings, please click on the "OK" (7) button; if you want to go back to the previous menu, click on the "Back" button.

3.3.6 Setup Procedure for Telstra Big Pond

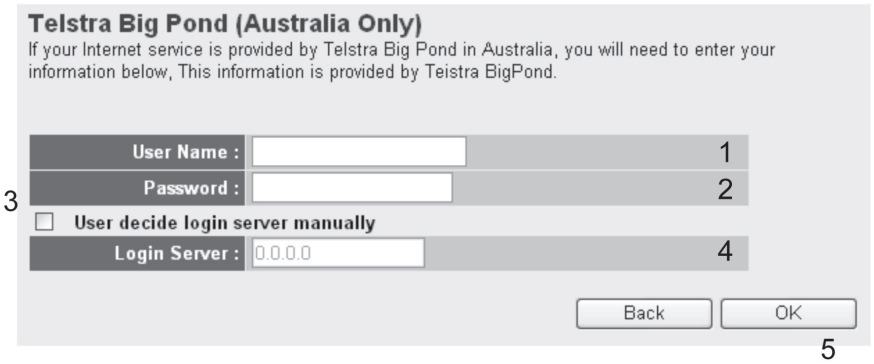


Figure 3-27. Telstra big pond setup.

This setting only works when you're using Telstra big pond's network service in Australia.

Table 3-7. Telstra big pond options.

Item	Description
User Name (1):	Type in the user name assigned by Telstra.
Password (2):	Type in the password assigned by Telstra.
User device login server manually (3):	Check this box to choose the login server by yourself.
Login Server (4):	Type in the login server's IP address here.

When you finish with all settings, click on the "OK" (5) button; if you want to go back to the previous menu, click on the "Back" button.

When all settings are finished, you'll see the following message displayed:

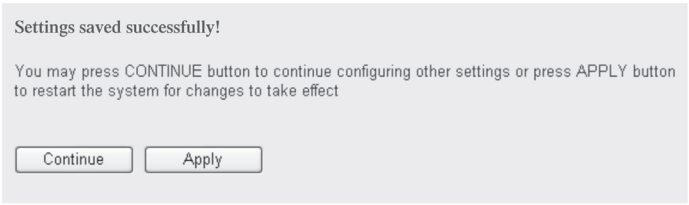

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 3-28. Settings saved successfully screen.

Click on the "Apply" button to prepare to restart the router, and you'll see this message:

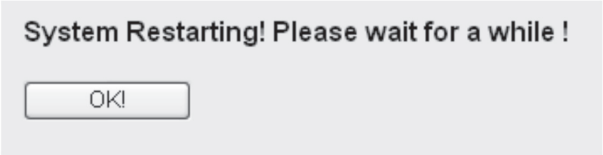


Figure 3-29. System restart screen.

Wait for about 30 seconds, then click on the "OK" button. You'll be back to the router management interface again, and the router is ready with new settings.

3.4 Basic Setup

In this section, you'll learn how to change the time zone, password, and remote management settings. Start your Web browser and log onto the router's Web management interface. Then click on the "General Setup" button on the left or click on the General Setup link at the upper-right corner of the Web management interface.

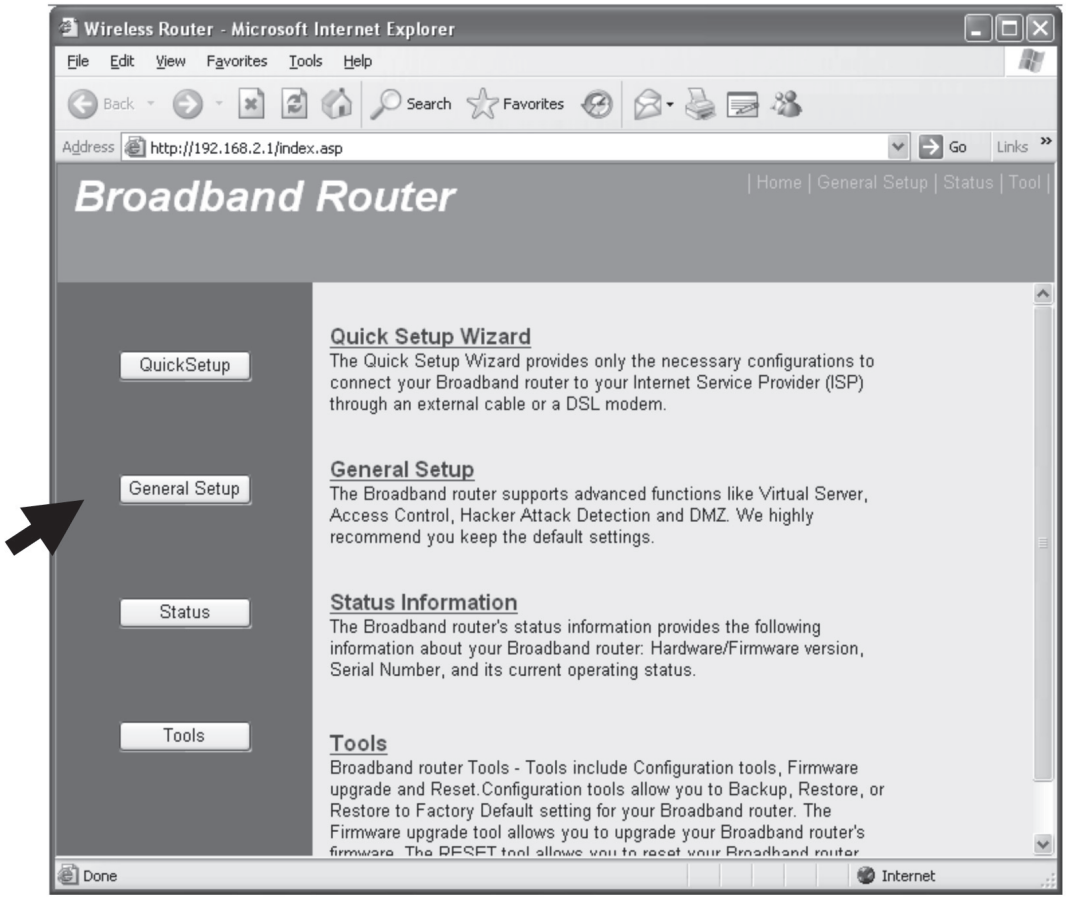

Wireless Router - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.2.1/index.asp
Go Links
Broadband Router
| Home | General Setup | Status | Tool |
QuickSetup
General Setup
Status
Tools
Quick Setup Wizard
The Quick Setup Wizard provides only the necessary configurations to connect your Broadband router to your Internet Service Provider (ISP) through an external cable or a DSL modem.
General Setup
The Broadband router supports advanced functions like Virtual Server, Access Control, Hacker Attack Detection and DMZ. We highly recommend you keep the default settings.
Status Information
The Broadband router's status information provides the following information about your Broadband router: Hardware/Firmware version, Serial Number, and its current operating status.
Tools
Broadband router Tools - Tools include Configuration tools, Firmware upgrade and Reset.Configuration tools allow you to Backup, Restore, or Restore to Factory Default setting for your Broadband router. The Firmware upgrade tool allows you to upgrade your Broadband router's
Done
Internet

Figure 3-30. Basic setup screen.

3.4.1 Time Zone and Time Auto-Synchronization

Follow the instructions below to set time zone and time auto-synchronization parameters:

Click on the "System" menu on the left of the Web management interface, then click on "Time Zone." Select the time zone from the Set time zone drop-down list, and input the IP address or host name of the time server. If you want to enable the daylight savings setting, check on the "Enable Function" box, and set the duration of daylight savings time. When you finish, click on the "Apply" button. You'll see the following message displayed:

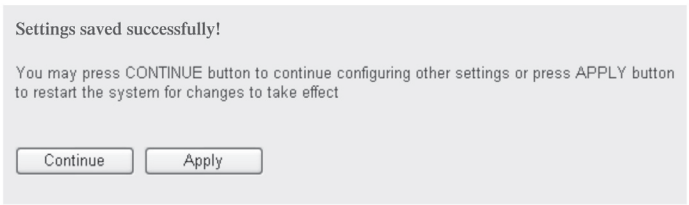

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 3- 31. Settings saved successfully screen.

Press "Continue" to save the settings and go back to the Web management interface; press "Apply" to save the settings made and restart the router so the settings will take effect after it reboots.

NOTE: You can refer to the instructions provided in Section 3.3, Using Quick Setup, for detailed descriptions on time zone settings.

3.4.2 Change the Management Password

The default password of this router is "1234," and it's displayed on the login prompt when accessed from the Web browser. There's a security risk if you don't change the default password, since everyone can see it. This is very important when you have the wireless function enabled.

To change the password, click on the "System" menu on the left of the Web management interface, then click on "Password Settings," and the following message will be displayed:

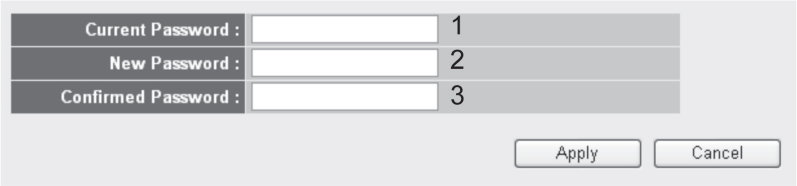


Figure 3-32. Change password screen.

Table 3-8. Change password options.

Item	Description
Current Password (1):	Input the current password here.
New Password (2):	Input the new password here.
Confirmed Password (3):	Input the new password here again.

When you finish, click on the "Apply" button. If you want to keep the original password unchanged, click on the "Cancel" button.

If the password you typed in New Password (2) and Confirmed Password (3) field are not the same, you'll see the following message:

Figure 3-33. Password not matched screen.

Retype the new password again if you see the message above.

If you see the following message:

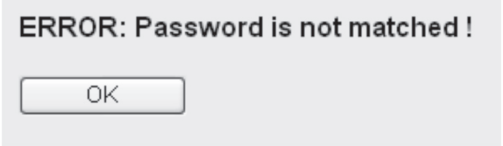


Figure 3-34. Password error screen.

The content in the Current Password field is wrong. Click on "OK" to go back to the previous menu, and try to input the current password again.

If the current and new passwords are entered correctly, after you click on "Apply," you'll be prompted to input your new password.

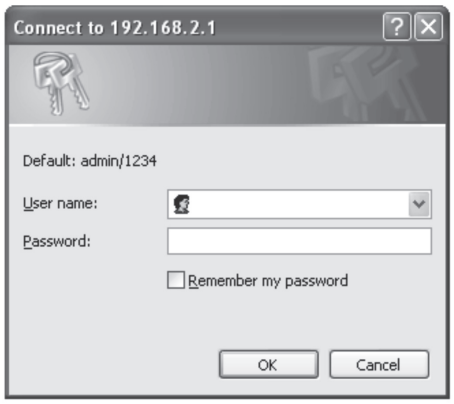


Figure 3-35. Enter password screen.

Use the new password to enter the Web management interface again, and you should be able to log in with the new password.

3.4.3 Remote Management

This router does not allow management access from the Internet to prevent possible security risks (especially when you defined a weak password or didn't change the default password). However, you can still manage this router from a specific IP address by enabling the Remote Management Function.

To do so, follow these instructions:

Click on the "System" menu on the left of the Web management interface, then click on "Remote Management," and the following message will be displayed:

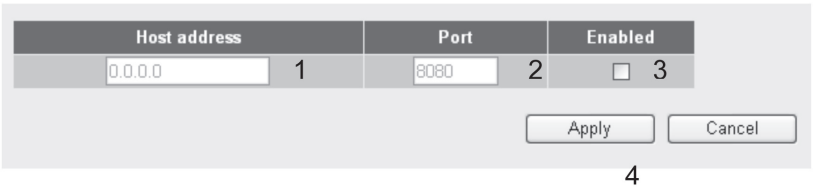


Figure 3-36. Set IP address for remote management.

Table 3-9. Remote management IP address options.

Item	Description
Host Address (1):	Input the IP address of the remote host you want to initiate management access.
Port (2):	Define the port number on which this router should expect an incoming request. If you're providing a Web service (default port number is 80), try to use another port number. You can use the default port setting 8080, or any integer between 1 and 65534.
Enabled (3):	Select the field to start the configuration.

When you finish with these settings, click on the "Apply" button, and you'll see the following message displayed on the Web browser:

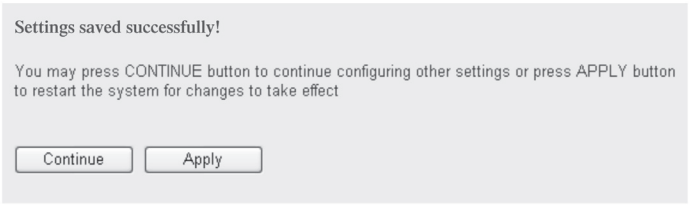

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 3-37. Settings saved successfully screen.

Press the "Continue" button to save the settings and go back to the Web management interface; press the "Apply" button to save the settings made and restart the router so the settings will take effect after it reboots.

NOTE: When you want to manage this router from another computer on the Internet, you have to input the router's IP address and port number. If your Internet service provider assigns you a static IP address, you won't have a problem. If the IP address your service provider assigns to you will vary every time you make an Internet connection, you will have a problem.

Either ask your service provider to give you a static IP address, or use dynamic IP to host name mapping services such as DDNS. Refer to Section 3.5.8, DDNS Client, for details.

NOTE: The default port number that the Web browser will use is "80." If the port setting on this page is not 80, you have to assign the port number in the Web browser's address bar manually. For example, if this router's IP address is 1.2.3.4, and the port number you set is 8888, you have to input the following address in the Web browser's address bar: "http://1.2.3.4:8888"

3.5 Setup Internet Connection (WAN Setup)

You can set up the Internet connection by using the Quick Setup menu described in Section 3.3. However, to set up WAN connections, you need to use the WAN configuration menu. You can also set advanced functions such as DDNS (Dynamic DNS) here.

To start the configuration, follow these instructions:

Click on the "WAN" menu on the left of the Web management interface, and the following screen will be displayed:

Select an Internet connection method depending on the type of connection you're using. You can either click the connection method on the left (1) or right (2). If you select the connection method on the right, click on the "More Configuration" button after you select a method.

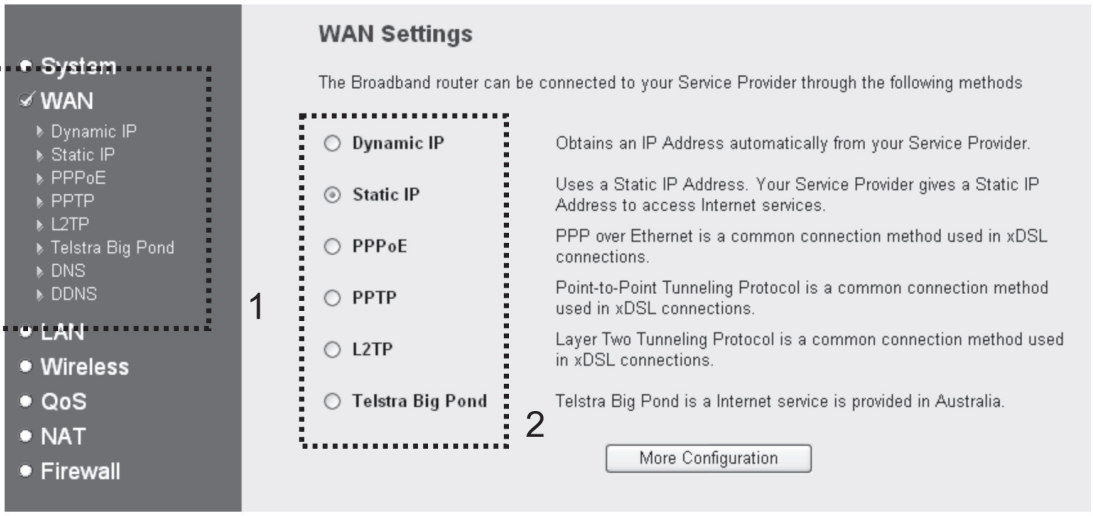


Figure 3-38. WAN setup screen.

- Dynamic IP: go to section 3.5.1
- Static IP: go to section 3.5.2
- PPPoE: go to section 3.5.3
- PPTP: go to section 3.5.4
- L2TP: go to section 3.5.5
- Telstra Big Pond: go to section 3.5.6
- DNS: go to section 3.5.7
- DDNS: go to section 3.5.8

3.5.1 Setup Procedure for Dynamic IP

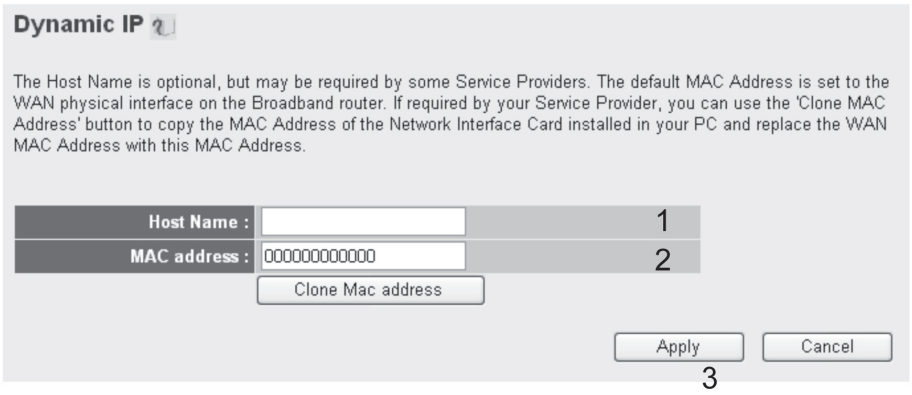

Dynamic IP
The Host Name is optional, but may be required by some Service Providers. The default MAC Address is set to the WAN physical interface on the Broadband router. If required by your Service Provider, you can use the 'Clone MAC Address' button to copy the MAC Address of the Network Interface Card installed in your PC and replace the WAN MAC Address with this MAC Address.
Host Name :
1
MAC address :
000000000000
2
Clone Mac address
Apply
Cancel
3

Figure 3-39. Dynamic IP setup screen.

Table 3-10. Dynamic IP options.

Item	Description
Host Name (1):	Type in your computer's host name. This is optional and only required if your service provider asks you to do so.
MAC Address (2):	Type in your computer's MAC address, if your service provider only permits computers with certain MAC addresses to access the Internet. If you're using the computer that's used to connect to the Internet via a cable modem, simply press the "Clone Mac address" button to fill the MAC address field with your computer's MAC address.

After you finish with the settings, please click on the "Apply" (3) button; if you want to remove any value you entered, click on the "Cancel" button.

After you click on the "Apply" button, the following message will be displayed:

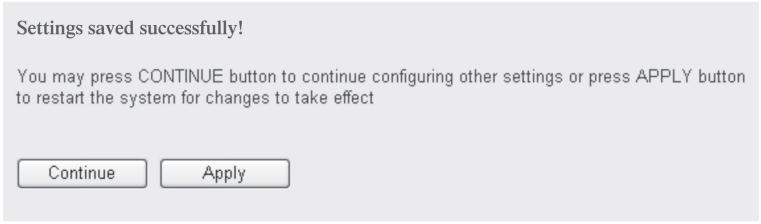

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 3-40. Settings saved successfully screen.

Click on the "Continue" (1) button to go back to the previous setup menu to continue with router setup, or click on the "Apply" button to reboot the router so the settings will take effect (please wait for about 30 seconds while the router reboots).

3.5.2 Setup Procedure for Static IP

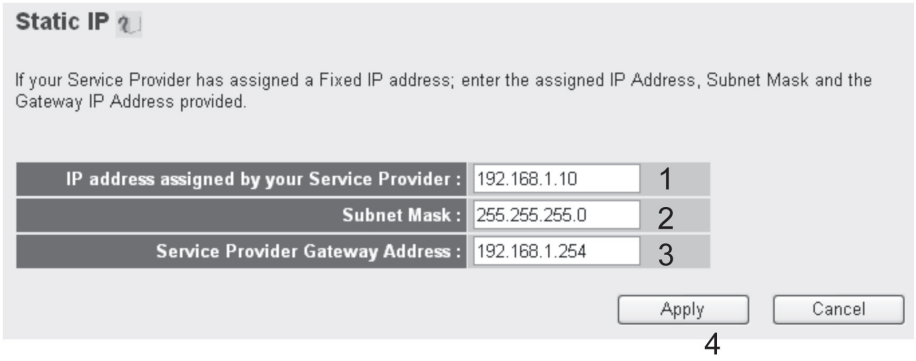


Figure 3-41. Static IP setup screen.

Table 3-11. Static IP options.

Iterm	Description
IP address assigned by your Service Provider (1):	Type in the IP address assigned by your service provider.
Subnet Mask (2):	Type in the subnet mask assigned by your service provider
Service Provider Gateway Address (3):	Type in the IP address of DNS server provided by your service provider.

After you finish with all settings, click on the "Apply" (4) button, and the following message will be displayed:

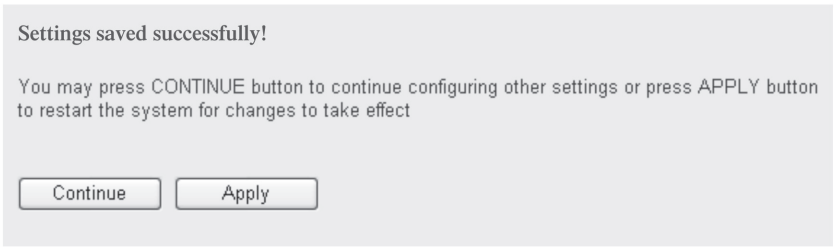

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 3-42. Settings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu to continue with other setup procedures, or click on the "Apply" button to reboot the router so the settings will take effect (please wait for about 30 seconds while the router reboots).

If you want to reset all settings on this page back to a previously saved value, click on the "Cancel" button.

3.5.3 Setup Procedure for PPPoE

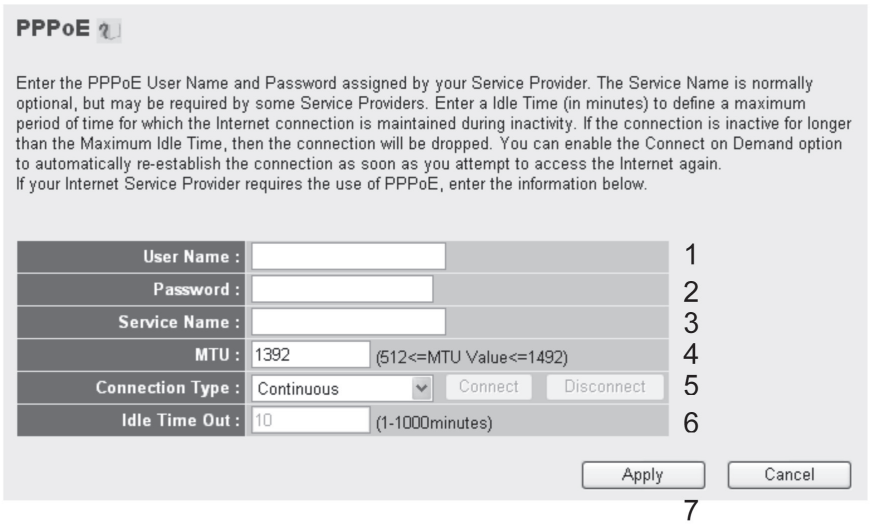

PPPoE
Enter the PPPoE User Name and Password assigned by your Service Provider. The Service Name is normally optional, but may be required by some Service Providers. Enter a Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, then the connection will be dropped. You can enable the Connect on Demand option to automatically re-establish the connection as soon as you attempt to access the Internet again.
If your Internet Service Provider requires the use of PPPoE, enter the information below.
User Name :
Password :
Service Name :
MTU : 1392 (512<=MTU Value<=1492)
Connection Type : Continuous Connect Disconnect
Idle Time Out : 10 (1-1000minutes)
Apply Cancel
1
2
3
4
5
6
7

Figure 3-43. PPPoE setup.

Table 3-12. PPPoE options.

Item	Description
User Name (1):	Input the user name assigned by your Internet service provider here.
Password (2):	Input the password assigned by your Internet service provider here.
Service Name (3):	Give a name to this Internet service; this is optional.
MTU (4):	Input the MTU value of your network connection here. If you don't know, use the default value.
Connection Type (5):	Select the type of Internet connection you want to use. Continuous – The connection will be always on. If the connection is interrupted, the router will re-connect automatically. Connect On-Demand – Only connect when you want to surf the Internet. Idle Time Out is set to stop the connection when the network traffic is not sending or receiving after an idle time. Manual – Select this option and you will see the Connect button and Disconnect button. Click on the "Connect" button and the router will connect to the ISP. If you want to stop the connection, click on the "Disconnect" button.
Idle Time Out (6):	If you selected the connection type as Connect-On-Demand, input the idle time out.

After you finish with the settings, click on the "Apply" (7) button and the following message will be displayed:

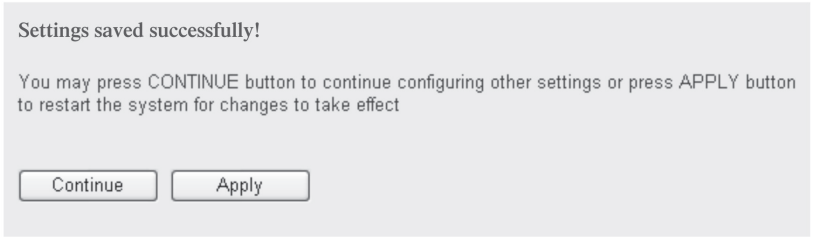

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 3-44. Settings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu or to continue with other setup procedures. Click on the "Apply" button to reboot the router so the settings will take effect (wait for about 30 seconds while router reboots).

To reset all settings on this page back to their previously saved values, click on the "Cancel" button.

3.5.4 Setup Procedure for PPTP

PPTP requires two kinds of settings: WAN interface setting (setup IP address) and PPTP setting (PPTP user name and password). Start at the WAN interface setting:

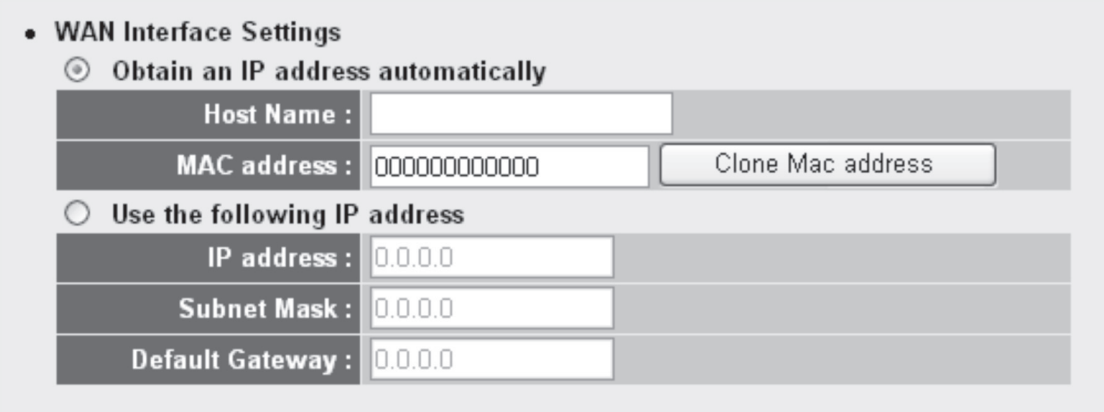


Figure 3-45. WAN interface settings screen.

Select how you obtain an IP address from your service provider here. Choose "Obtain an IP address automatically" (equal to DHCP, refer to the Cable Modem section 3.3.1), or "Use the following IP address" (that is, static IP address).

WAN interface settings must be correctly set, or the Internet connection will fail even if the PPTP settings are correct. Contact your Internet service provider if you don't know how you should fill in these fields.

Go to the PPTP settings section:

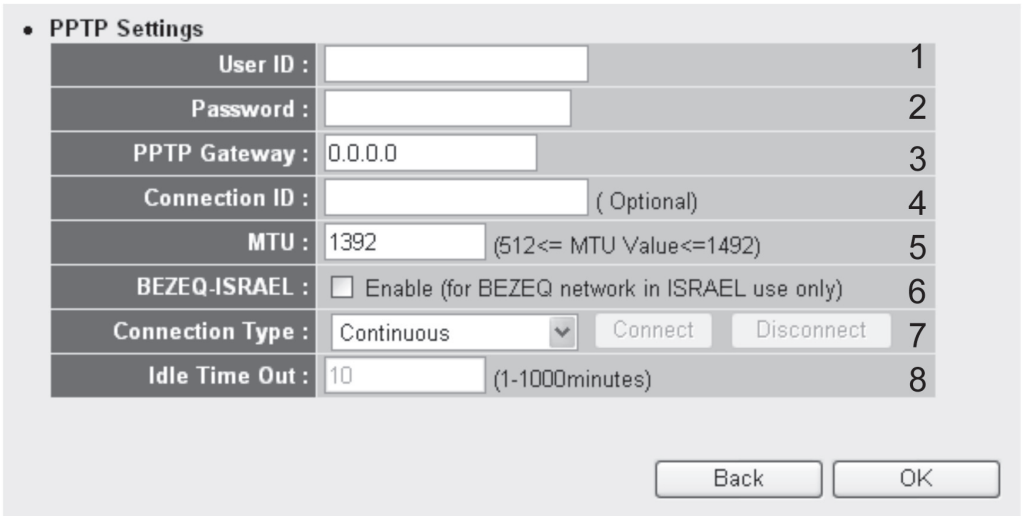


Figure 3-46. PPTP settings screen.

Table 3-13. PPTP settings options.

Item	Description
User ID (1):	Input the user ID (user name) assigned by your Internet service provider here.
Password (2):	Input the password assigned by your Internet service provider here.
PPTP Gateway (3):	Input the PPTP gateway's IP address assigned by your Internet service provider here.
Connection ID (4):	Input the connection ID here; this is optional and you can leave it blank.
MTU (5):	Input the MTU value of your network connection here. If you don't know it, you can use the default value.
BEZEQ-ISRAEL (6):	If you are connecting to the BEZEQ network in Israel, enable this function.
Connection type (7):	Select the type of Internet connection you want to use; refer to Section 3.5 for detailed descriptions.
Idle Time Out (8):	Input the idle time out of the Internet connection you want to use, and refer to Section 3.3.3 for detailed descriptions.

When you finish with the settings, click on the "OK" (9) button; if you want to go back to the previous menu, click on the "Back" button.

3.5.5 Setup Procedure for L2TP

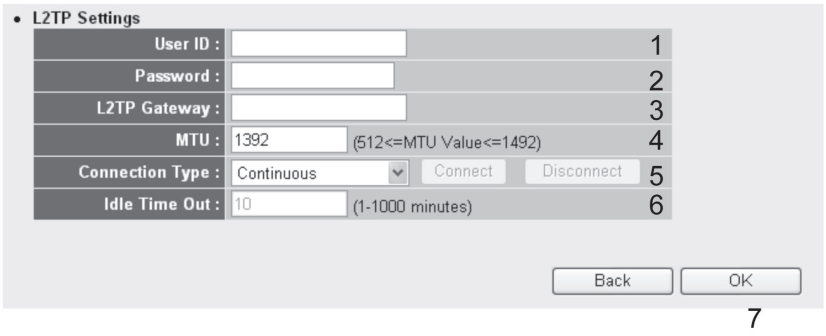


Figure 3-47. L2TP settings.

Table 3-14. L2TP settings options.

Item	Description
User ID (1):	Input the user ID (user name) assigned by your Internet service provider here.
Password (2):	Input the password assigned by your Internet service provider here.
L2TP Gateway (3):	Input the PPTP gateway's IP address assigned by your Internet service provider here.
MTU (4):	Input the MTU value of your network connection here. If you don't know, you can use the default value.
Connection type (5):	Select the connection type of the Internet connection you want to use; refer to Section 3.5 for detailed descriptions.
Idle Time Out (6):	Input the idle time out of the Internet connection you want to use, and refer to Section 3.3.3 for detailed descriptions.

When you finish with the settings, click on the "OK" (7) button. If you want to go back to the previous menu, click on the "Back" button.

3.5.6 Setup Procedure for Telstra Big Pond

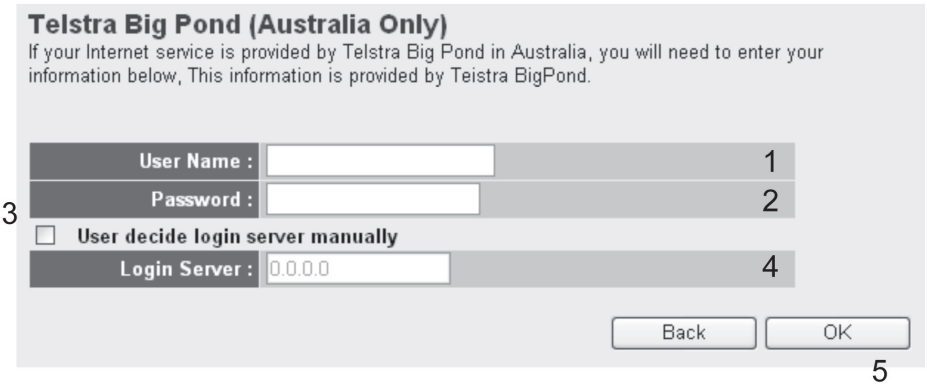


Figure 3-48. Telstra big pond setup.

This setting only works when you're using Telstra Big Pond's network service in Australia. You need to input the parameters described in Table 3-15.

Table 3-15. Telstra big pond options.

Item	Description
User Name (1):	Input the user name assigned by Telstra.
Password (2):	Input the password assigned by Telstra.
User device login server manually (3):	Check this box to choose the login server by yourself.
Login Server (4):	Input the IP address of the login server here.

When you finish with all settings, click on the "OK" (5) button; if you want to go back to the previous menu, click on the "Back" button.

3.5.7 Setup Procedure for DNS

If you select Dynamic IP or PPPoE as the Internet connection method, at least one DNS server's IP address should be assigned automatically. However, if you have a preferred DNS server or your service provider didn't assign the DNS server's IP address, you can input the DNS server's IP address here.

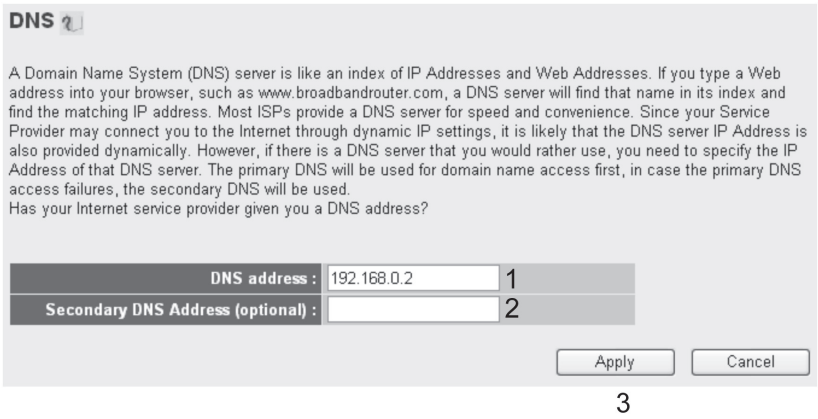

DNS
A Domain Name System (DNS) server is like an index of IP Addresses and Web Addresses. If you type a Web address into your browser, such as www.broadbandrouter.com, a DNS server will find that name in its index and find the matching IP address. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect you to the Internet through dynamic IP settings, it is likely that the DNS server IP Address is also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP Address of that DNS server. The primary DNS will be used for domain name access first, in case the primary DNS access failures, the secondary DNS will be used.
Has your Internet service provider given you a DNS address?
DNS address :
192.168.0.2
1
Secondary DNS Address (optional) :
2
Apply
Cancel
3

Figure 3-49. DNS setup screen.

Table 3-16. DNS setup options.

Item	Description
DNS Address (1):	Input the DNS server's IP address provided by your service provider.
Secondary DNS Address (2):	Input another DNS server's IP address provided by your service provider (this is optional).

NOTE: Enter only the IP address here; DO NOT use the DNS server's hostname because only numeric characters and dots are accepted.

10.20.30.40.....Correct

After you finish the settings, please click on the "Apply" (3) button and the following message will be displayed:

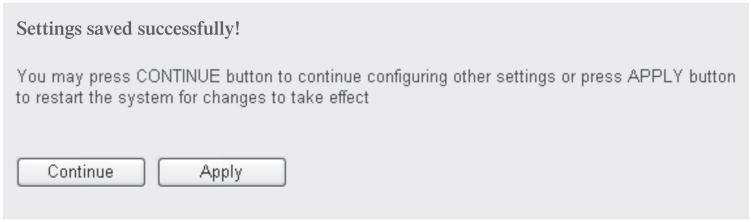

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 3-50. Settings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu or to continue with other setup procedures. Click on the "Apply" button to reboot the router so the settings will take effect (please wait for about 30 seconds while the router reboots).

If you want to reset all settings on this page back to previously saved values, click on the "Cancel" button.

3.5.8 Setup Procedure for DDNS

DDNS (Dynamic DNS) is an IP-to-Hostname mapping service for those Internet users who don't have a static (fixed) IP address. It will be a problem when a user wants to provide services to other users on Internet because their IP address will vary every time when connected to Internet, and the other user will not know the IP address they're using at a certain time.

This router supports several service providers' DDNS services, for example:

DynDNS (http://www.dyndns.org)

TZO (http://www.tzo.com)

Go to one of the DDNS service provider's Web pages listed on the previous page, and get a free DDNS account.

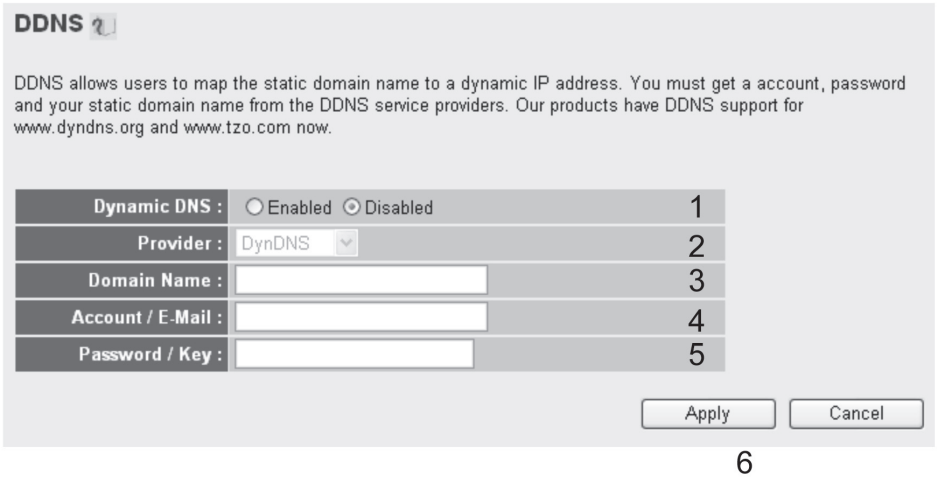


Figure 3-51. DDNS settings screen.

Table 3-17. DDNS options.

Item	Description
Dynamic DNS (1):	If you want to enable DDNS function, select "Enabled;" otherwise, select "Disabled."
Provider (2):	Select your DDNS service provider here.
Domain Name (3):	Input the domain name you've obtained from the DDNS service provider.
Account/E-Mail (4):	Input the DDNS registration's account or e-mail.
Password/Key (5):	Input the DDNS service password or key.

After you finish with the settings, click on the "Apply" (6) button and the following message will be displayed:

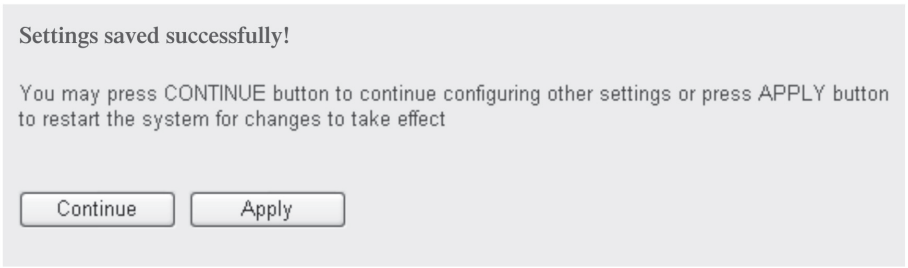

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 3-52. Settings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu or to continue with other setup procedures. Click on the "Apply" button to reboot the router so the settings will take effect (please wait for about 30 seconds while the router reboots).

To reset all settings in this page back to previously saved values, click on the "Cancel" button.

3.6 Wired LAN Configurations

Before all computers using wired Ethernet connections (that is, those computers connected to this router's LAN Ports 1 to 4 via Ethernet cable) can communicate with each other and access the Internet, they must have a valid IP address.

There are two ways to assign IP addresses to computers: static IP address (set the IP address for every computer manually), and dynamic IP address (IP address of computers will be assigned by router automatically). We recommend using dynamic IP addresses for most computers. It will save time on setting IP addresses for every computer, especially when there are a lot of computers in your network. For servers and network devices that will provide services to other computers and users on the Internet, use a static IP address so that other computers can locate the server.

Suggestions for IP address numbering:

If you have no idea how to define an IP address plan for your network, read the following suggestions:

1. A valid IP address has four fields: a.b.c.d. For most home and company users, we recommend using "192.168.c.d," where c is an integer between 1 and 254. This router can work with up to 253 clients, so you can set the d field of the router's IP address as 1 or 254 (or any number between 1 and 254), and pick a number between 0 and 254 for field c.
2. In most cases, you should use "255.255.255.0" as the subnet mask, which allows up to 253 clients.
3. All servers and network devices that will provide services to other people (such as Internet service, print service, and file service) should use static IP addresses. Give each of them a unique number between 1 and 253, and maintain a list, so that everyone can locate those servers easily.
4. Computers that are not dedicated to provide specific service to others should use dynamic IP addresses.

If you don't understand the descriptions listed above, refer to the recommended setup values below.

Follow these instructions to set wired LAN parameters:

Click on the LAN menu on the left of web management interface. There are three setup groups here: LAN IP, DHCP Server, and Static DHCP Leases Table.

3.6.1 LAN IP Section

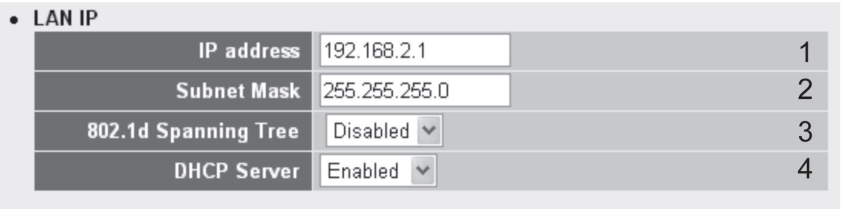


Figure 3-53. LAN IP settings screen.

Table 3-18. LAN IP options.

Item	Description
IP address (1):	Input the router's IP address.
Subnet Mask (2):	Input the network's subnet mask.
802.1d Spanning Tree (3):	If you want to activate the 802.1d Spanning Tree function, select "Enabled" for setup item 802.1d Spanning Tree, or set it to "Disabled."
DHCP Server (4):	If you want to activate this router's DHCP server function, select "Enabled." Otherwise, set it to "Disabled."

Recommended values if you don't know what to use:

IP address: 192.168.2.1

Subnet mask: 255.255.255.0

802.1d Spanning Tree: Disabled

DHCP server: Enabled

3.6.2 DHCP Server

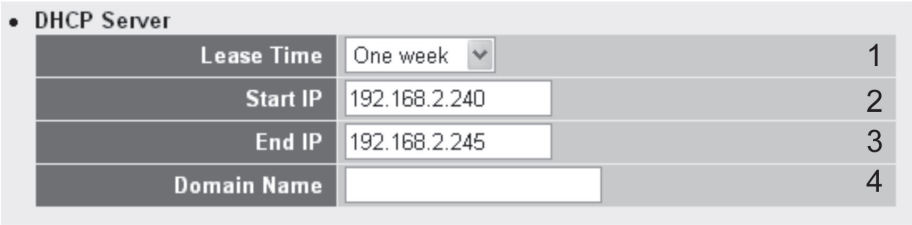


Figure 3-54. DHCP screen.

These settings are only available when DHCP Server in the LAN IP section is Enabled.

Table 3-19. DHCP options.

Item	Description
Lease Time (1):	Choose a lease time (the duration that every computer can keep a specific IP address) for every IP address assigned by this router from the drop-down menu.
Start IP (2):	Input the start IP address of the IP range.
End IP (3):	Input the end IP address of the IP range.
Domain Name (4):	If you want, you can also optionally input the domain name for your network. This is optional.

Recommended values if you don't know what to use:

Lease time: Two weeks or forever if you have less than 20 computers.

Start IP: 192.168.2.100

End IP: 192.168.2.200

Domain name: (leave it blank)

NOTES: 1. The last field (d field)'s number End IP must be greater than Start IP, and can't be the same as the router's IP address.

2. The former three IP address fields (Start IP, End IP, and IP Address [a, b, and c fields] should be the same).

3. These settings will affect wireless clients, too.

3.6.3 Static DHCP Leases Table

This function allows you to assign a static IP address to a specific computer forever, so you don't have to set the IP address for a computer, and still use a DHCP server. A maximum of 16 static IP addresses can be assigned here.

If you set "Lease Time" to forever in the DHCP Server section, you can also assign an IP address to a specific computer permanently. However, you will not be able to assign a certain IP address to a specific computer, since IP addresses will be assigned in random order.

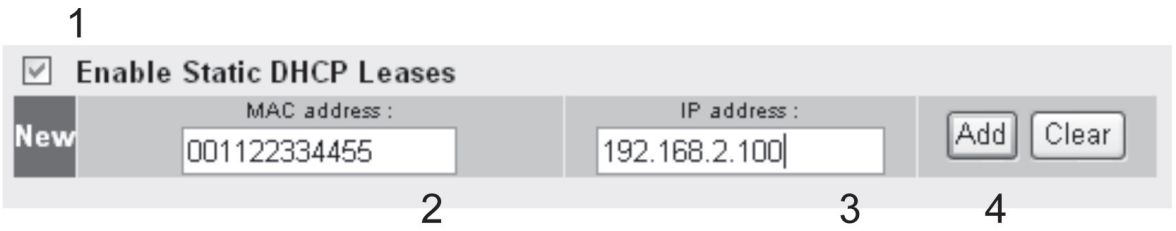


Figure 3-55. Enable static DHCP leases screen.

Table 3-20. Enable static DHCP leases screen options.

Item	Description
Enable Static DHCP Leases (1):	Check this box to enable this function; otherwise, uncheck it to disable this function.
MAC Address (2):	Input the MAC address of the computer or network device (total of 12 characters, with characters ranging from 0 to 9, and from a to f, such as '001122aabbcc').
IP address (3):	Input the IP address you want to assign to this computer or network device.
Add (4):	After you input the MAC address and IP address pair, click this button to add the pair to the static DHCP leases table.

If you want to remove all characters you just entered, click on the "Clear" button.

After you click on the "Add" button, the MAC address and IP address mapping will be added to the Static DHCP Leases Table.

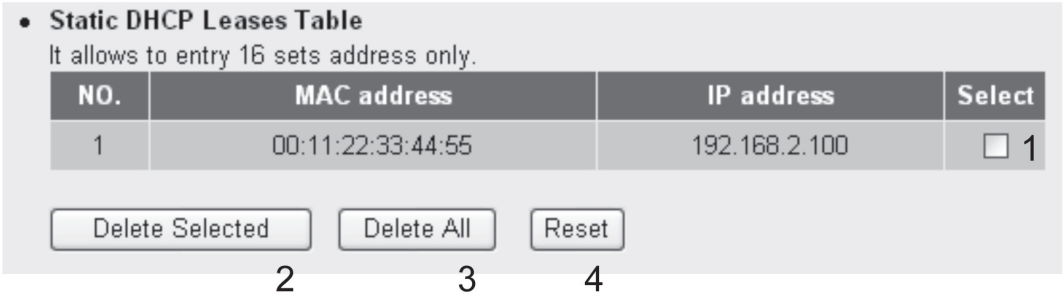


Figure 3-56. Static DHCP leases table.

If you want to delete a specific item, check the Select box of a "MAC address" and "IP address" mapping (1), then click on the "Delete Selected" (2) button. If you want to delete all mappings, click on the "Delete All" (3) button. If you want to deselect all mappings, click on the "Reset" (4) button.

After you finish all LAN settings, click on the "Apply" button on the bottom of this page. The following message will be displayed on your Web browser:

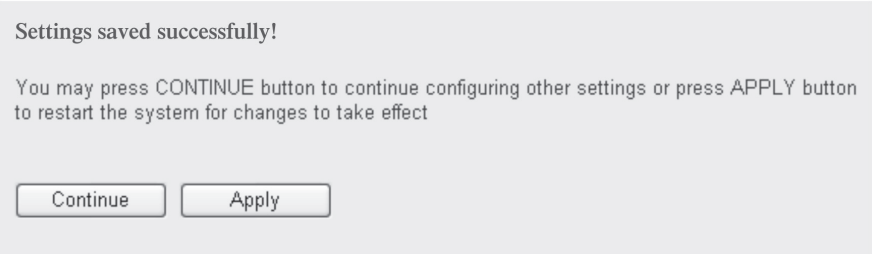

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 3-57. Settings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu to continue with router setup. Click on the "Apply" button to reboot the router so the settings will take effect (please wait for about 30 seconds while the router reboots).

3.7 Wireless LAN Configurations

If your computer, PDA, game console, or other network device is equipped with a wireless network interface, you can use the router's wireless function to let the device connect to the Internet and share resources with other computers with wired-LAN connection. You can also use the built-in security functions to protect your network from malicious intruders.

To set wireless parameters, click on the "Wireless" menu on the left of the Web management interface, and the following message will be displayed: "You must enable the router's wireless function, or the router's wireless interface will not function." Select "Enable" (1), then click on the "Apply" (2) button.

To disable wireless function, select "Disable" (3), then click on the "Apply" (2) button.

Wireless Settings
The gateway can be quickly configured as a wireless access point for roaming clients by setting the access identifier and channel number. It also supports data encryption and client filtering.
Enable or disable Wireless module function : Enable Disable
1
3
Apply
2

Figure 3-58. Wireless settings screen.

After you click on the "Apply" button, the following message will be displayed on your Web browser:

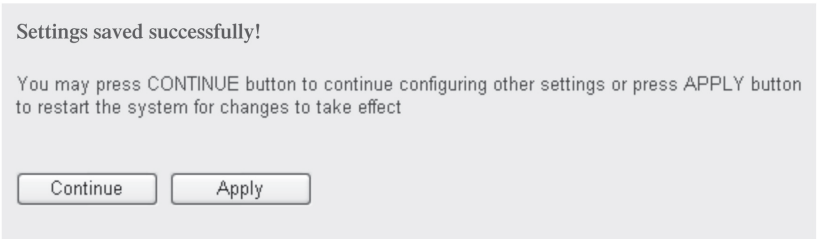

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 3-59. Settings saved successfully screen.

Click on the "Continue" button to go to back to the previous setup menu to continue with other setup procedures. Or, click on the "Apply" button to reboot the router so the settings will take effect (please wait for about 30 seconds while the router reboots).

3.7.1 Basic Wireless Settings

Click on the "Wireless" menu on the left of the web management interface, then click on "Basic Settings." The following message will be displayed:

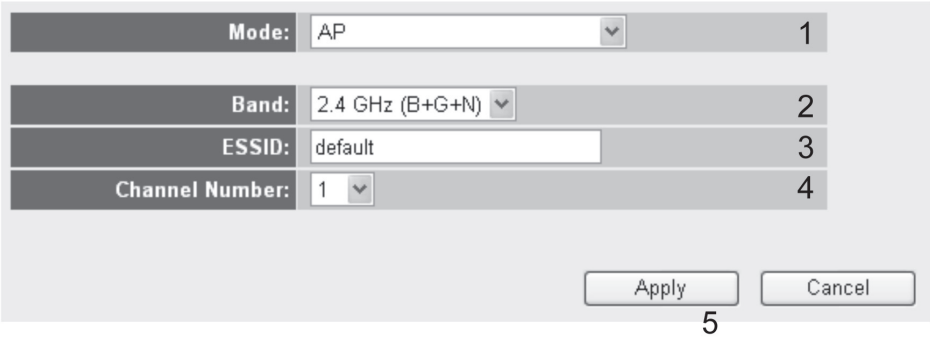


Figure 3-60. Basic wireless settings screen.

This wireless router works in six modes:

1. AP: Standard wireless AP (access point).
2. Station-Infrastructure: Connect the router to an Ethernet device such as TV, game player, HDD, or DVD to enable the Ethernet device to be a wireless station.
3. AP Bridge-Point to Point: Connect this router ro another wireless router, to expand the network.
4. AP Bridge-Point to Multipoint: Connect this router to up to four other wireless routers, to expand the network.
5. AP Bridge-WDS: Connect this router to up to four WDS-capable wireless routers, to expand the network.
6. Universal Repeater: The router can act as a station and an AP at the same time. It can use the station function to connect to a root AP and use the AP function to service all wireless stations within its coverage area.

NOTE: For AP bridge point-to-point and AP bridge point-to-multipoint, the wireless router operates only in wireless bridge dedicated mode. The wireless router is only used to expand the range of the network, and no wireless clients can be accepted. To use your wireless router to expand the range of your network and also accept wireless clients, select "AP bridge-WDS" or "universal repeater" mode.

Select a proper operation mode to use from the Mode drop-down menu (1), and continue with other operation-mode-specific settings:

Setup Procedure for AP

Select the radio band you want to use from the "Band" dropdown menu (2), and the following message will be displayed:

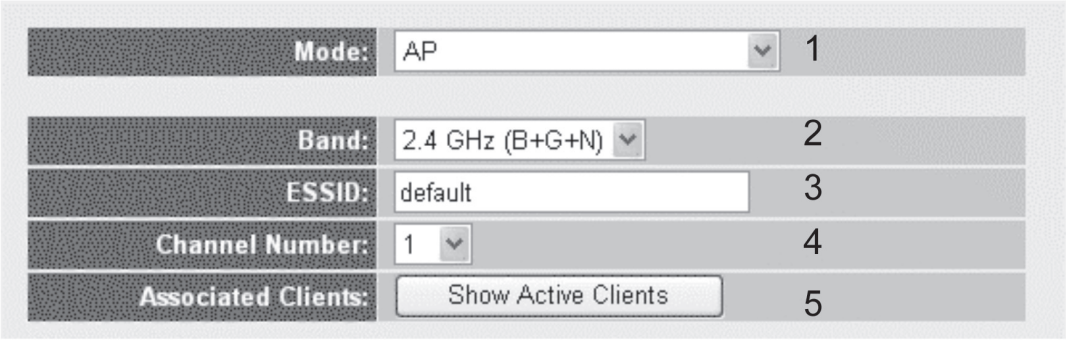


Figure 3-61. AP setup screen.

Table 3-21. AP setup options.

Item	Description
Band (2):	Select the radio band from the following options: 2.4 GHz (B): 2.4 GHz band, only allows the 802.11b wireless network client to connect to this router. The maximum transfer rate is 11 Mbps. 2.4 GHz (N): 2.4 GHz band, only allows the 802.11n wireless network client to connect to this router. The maximum transfer rate is 150 Mbps. 2.4 GHz (B+G): 2.4 GHz band, only allows the 802.11b and 802.11g wireless network client to connect to this router. The maximum transfer rate is 11 Mbps for 802.11b clients and 54 Mbps for 802.11g clients. 2.4 GHz (B+G+N): 2.4 GHz band, only allows the 802.11b, 802.11g, and 802.11n wireless network client to connect to this router. The maximum transfer rate is 11 Mbps for 802.11b clients, 54 Mbps for 802.11g clients, and 150 Mbps for 802.11n clients. *NOTE: For 802.11b and 802.11g mode, the signals can be transmitted only by antenna 1 (the antenna in the right side of the rear panel).* *For 802.11n mode, the router operates in a 2T2R spacial multiplexing MIMO configuration. Two antennas are for signal transmitting and two antennas are for signal receiving.*
ESSID (3):	This is the wireless router's name. Type up to 32 alphanumerical characters here. ESSID identifies your own wireless router from others when there are other wireless routers in the same area. The default is SSID. We recommend that you change the default ESSID value to one that's meaningful to you, such as myhome, office_room1, etc.

Table 3-21 (continued). AP setup options.

Item	Description
Channel Number (4):	Select a channel from the Channel Number drop-down list. Available channel numbers are 1 to 13 for European countries and 1 to 11 for the U.S. Choose any channel number you want to use; almost all wireless clients can locate the channel you're using automatically without any problem. However, it's still useful to remember the channel number you use, since some wireless clients support manual channel number select, and this would help when there is a radio communication problem.
Associated Clients (5):	Click on the "Show Active Clients" button, then an Active Wireless Client Table will pop up. You can see the status of all active wireless stations that are connecting to the access point.

NOTE: If you don't have a special reason to limit the type of allowed wireless client, we recommend that you choose 2.4 GHz (B+G+N) for maximum wireless compatibility.

TIP: You can try to change a channel number to another one if your think the data transfer rate is too slow. Other routers might be using the same channel, which will disturb the radio communication between the wireless client and the wireless radio.

Setup Procedure for Station-Infrastructure

In this mode, you can connect the router to an Ethernet device, such as a TV, game player, HDD, or DVD, to enable the Ethernet device to be a wireless station and join a wireless network through an access point or AP router.

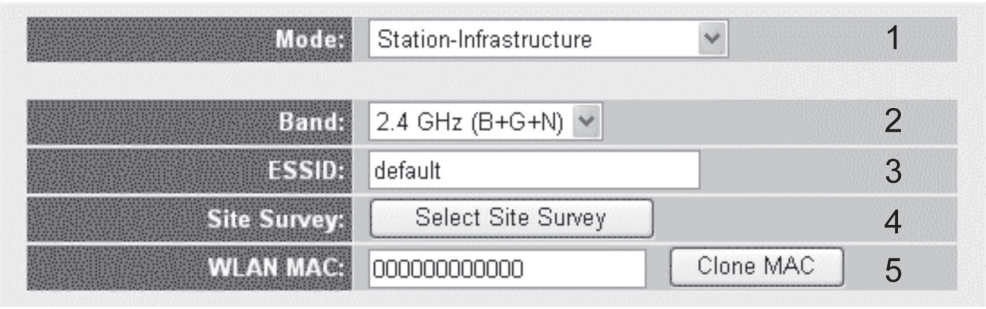


Figure 3-62. Station-Infrastructure screen.

Table 3-22. Station infrastructure options.

Item	Description
Band (2):	Select the band you want to use.
ESSID (3):	This is the wireless network's name. Type the SSID of the network you want to connect here.
Site Survey (4):	When you use this wireless router as a wireless station for an Ethernet network device to have wireless capability, you have to associate it with a working access point. Click on the "Select Site Survey" button, then a Wireless Site Survey Table will pop up. It will list all available access points nearby. You can select one access point in the table and it will join the wireless LAN through this access point.
WLAN MAC (5):	For some applications, you may need to designate a specific MAC address for the router. Enter the MAC address here. If you are connecting the router to a computer, simply press the "Clone Mac address" button to fill the MAC address field with your computer's MAC address.

Setup Procedure for AP Bridge-Point to Point

In this mode, you can connect your wireless router to another wireless router, combining two access points to expand the wireless network. All clients (wired only—AP will not accept wireless clients in this mode) of the two wireless routers will think they're on the same physical network. This function is very convenient when you need to connect two networks between two buildings.

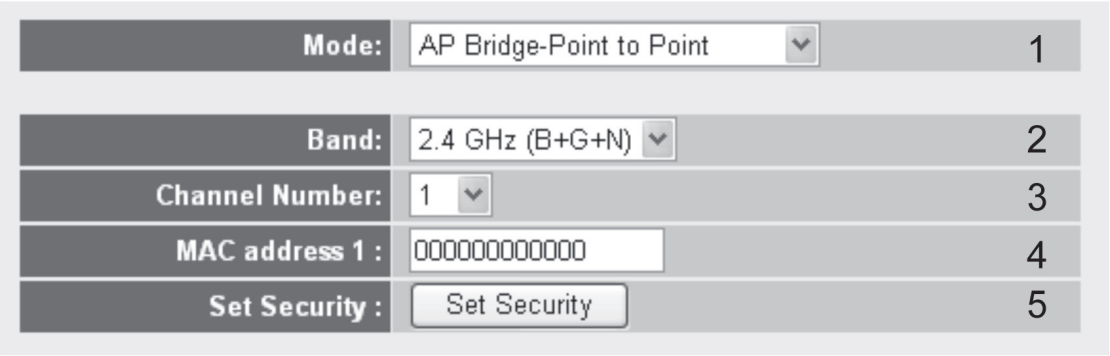


Figure 3-63. AP Bridge Point-to-Point screen.

Table 3-23. AP Bridge Point-to-point screen options.

Item	Description
Band (2):	Select the band you want to use. Two wireless routers must use the same setting.
Channel Number (3):	Select the channel you want to use,. Two wireless routers must use the same setting.
MAC address (4):	Input another wireless router's MAC address.
Set Security (5):	Click to set security settings for this connection. (Go to Section 3.7.3. Wireless Security, for detailed instructions).

Setup Procedure for AP Bridge-Point to Multi-Point

In this mode, you can connect your wireless router with at least four wireless routers to expand the scope of the wireless network. All clients (wired only—AP will not accept wireless clients in this mode) of the wireless routers will think they're on the same physical network.

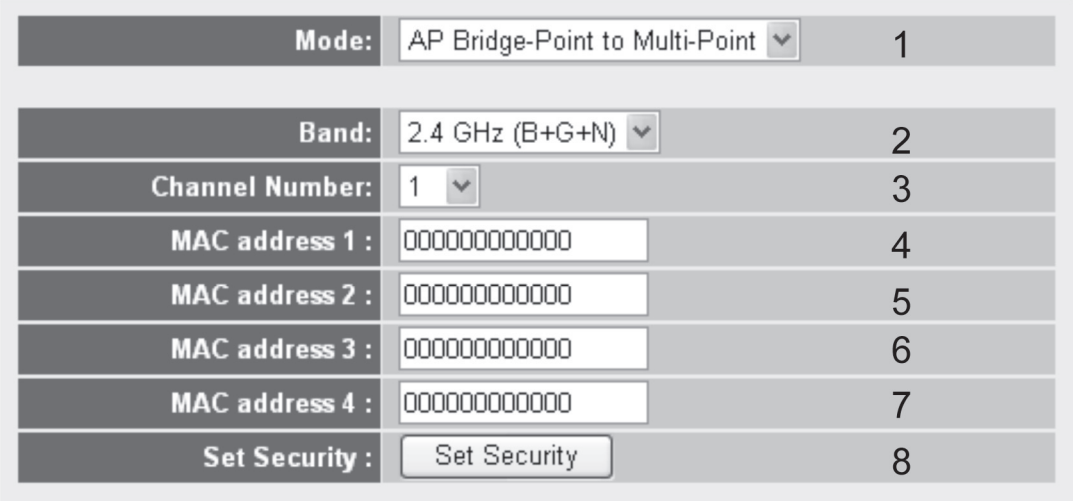


Figure 3-64. AP bridge-point-to-multipoint setup screen.

Table 3-24. AP bridge-point-to-multipoint options.

Item	Descriiption
Band (2):	Select the band you want to use. All the wireless routers must use the same setting.
Channel Number (3):	Select the channel you want to use. All the wireless routers must use the same setting.
MAC address 1 to 4 (4–7):	Input the other wireless routers' MAC addresses.
Set Security (8):	Click to set security settings for this connection (Go to Section 3.7.3, Wireless Security for detailed instructions).

Setup Procedure for AP Bridge—WDS

In this mode, you can expand the scope of your network by combining up to four other access points together. Every access point can still accept wireless clients.

NOTE: For WDS mode, the output signal is the same as that of the normal AP mode.

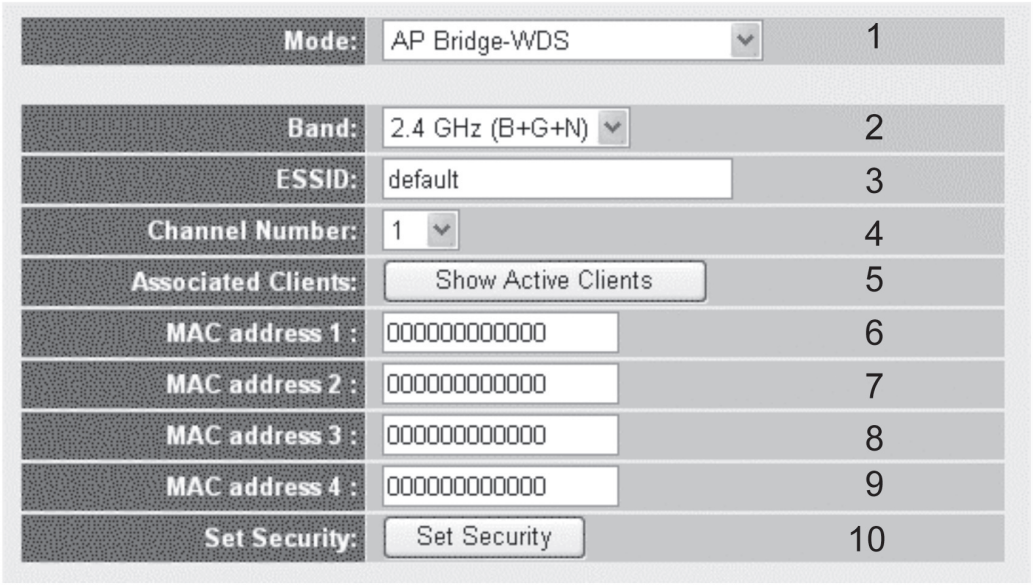


Figure 3-65. AP Bridge—WDS setup.

Table 3-25. AP bridge WDS options.

Item	Description
Band (2):	Select the band you want to use. All the wireless routers must use the same setting.
ESSID (3):	Input your wireless router's ESSID. The setting should be the same as other wireless routers for convenient roaming.
Channel Number (4):	Select the channel you want to use. All the wireless routers must use the same setting.
Associated Clients (5):	Click on the "Show Active Clients" button, then an "Active Wireless Client Table" will pop up. You can see the status of all active wireless stations that are connecting to the access point.
MAC address 1 to 4 (6–9):	Input the MAC address of other wireless routers.
Set Security (10):	Click to set security settings for this connection (go to Section 3.7.3, Wireless Security for detailed instructions).

Setup Procedure for Universal Repeater

In this mode, the router can act as a wireless repeater. It can be configured as a station and an AP at the same time. It uses the station function to connect to a root AP and uses the AP function to service all wireless stations within its coverage area.

NOTE: For repeater mode, this router will demodulate the received signal, checking if the signal is noise for the operating network. Then the signal is modulated and amplified again. This mode's output power is the same as that of WDS and normal AP mode.

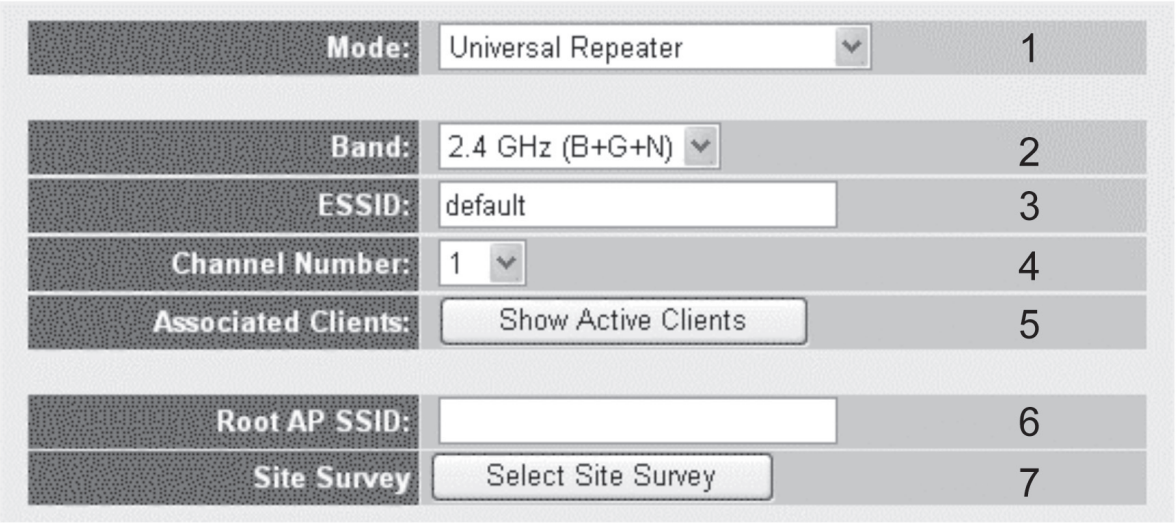


Figure 3-66. Universal repeater mode setup.

Table 3-26. Universal repeater mode options.

Item	Description
Band (2):	Select the band you want to use. All the wireless routers must use the same setting.
ESSID (3):	This is the wireless router's name. Type up to 32 alphanumeric characters here.. ESSID identifies your own wireless router from others when there are other wireless routers in the same area. The default SSID is "default." We recommend changing the default ESSID value to one that is meaningful to you, like myhome, office_room1, etc.
Channel Number (4):	Select the channel you want to use. All the wireless clients must use the same setting.
Associated Clients (5):	Click on the "Show Active Clients" button, then an "Active Wireless Client Table" will pop up. You can see the status of all active wireless stations that are connecting to the access point.
Root AP SSID (6):	In universal repeater mode, this device can act as a station to connect to a root AP. Assign the root AP's SSID here or click on the "Select Site Survey" button to choose a root AP.
Site Survey (7):	Click on the "Select Site Survey" button, then a "Wireless Site Survey Table" will pop up. It will list all available access points nearby. Select one access point in the table and the router will join the wireless LAN through this access point.

After you finish the wireless setting, click on the "Apply" button. The following message will be displayed:

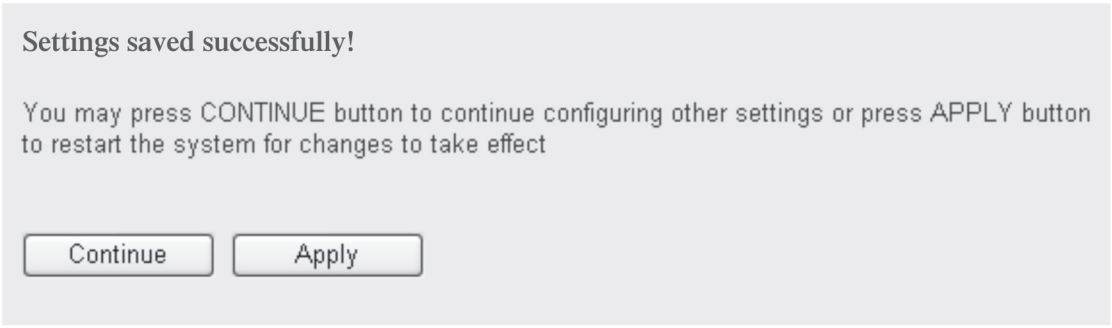

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 3-67. Settings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu to continue with router setup. Click on the "Apply" button to reboot the router so the settings will take effect (wait for about 30 seconds while the router reboots).

3.7.2 Advanced Wireless Settings

This router provides some advanced control of wireless parameters. If you want to configure these settings, click on the "Wireless" menu on the left of Web management interface, then click on "Advanced Settings." The following message will be displayed:

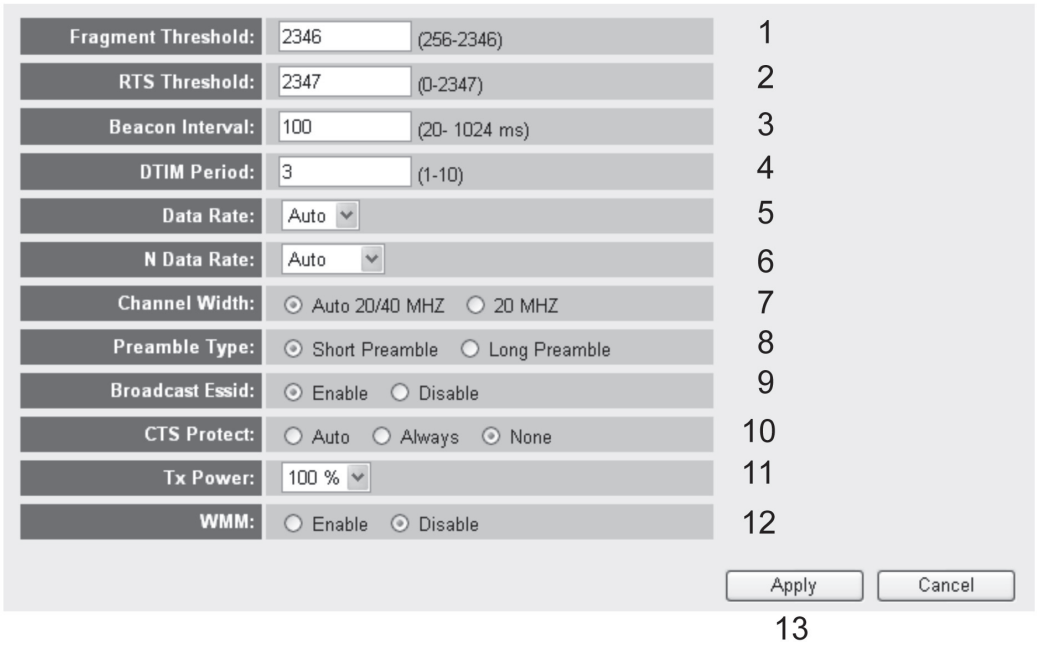

Fragment Threshold: 2346 (256-2346) 1
RTS Threshold: 2347 (0-2347) 2
Beacon Interval: 100 (20- 1024 ms) 3
DTIM Period: 3 (1-10) 4
Data Rate: Auto 5
N Data Rate: Auto 6
Channel Width: Auto 20/40 MHZ 20 MHZ 7
Preamble Type: Short Preamble Long Preamble 8
Broadcast Essid: Enable Disable 9
CTS Protect: Auto Always None 10
Tx Power: 100 % 11
WMM: Enable Disable 12
Apply Cancel
13

Figure 3-68. Advanced wireless settings screen.

Table 3-27. Advanced wireless settings options.

Item	Description
Fragment Threshold (1):	Set the wireless radio's fragment threshold. Do not modify the default value if you don't know what it is. The default value is "2346."
RTS Threshold (2):	Set the wireless radio's RTS threshold. Do not modify the default value if you don't know what it is. The default value is "2347."
Beacon Interval (3):	Set the wireless radio's beacon interval. Do not modify the default value if you don't know what it is. The default value is "100."
DTIM Period (4):	Set the wireless radio's DTIM period. Do not modify the default value if you don't know what it is. The default value is "3."
Data Rate (5):	Set the wireless data transfer rate to a certain value. Since most wireless devices will negotiate with each other and pick a proper data transfer rate automatically, it's not necessary to change this value unless you know what will happen after modification.
N Data Rate (6):	Same as above, but only for 802.11n clients.
Channel Width (7):	Set the wireless radio's channel width. Do not modify the default value if you don't know what it is. The default setting is "Auto 20/40 MHz."
Preamble Type (8):	Set the preamble type. Do not modify the default value if you don't know what it is. The default setting is "Short Preamble."
Broadcast ESSID (9):	Decide if the wireless router will broadcast its own ESSID or not. You can hide your wireless router's ESSID (set the option to "Disable"), so only people who know your wireless router's ESSID can connect to it.
CTS Protect (10):	Enabling this setting will reduce the chance of radio signal collisions between 802.11b and 802.11g/n wireless access points. We recommend setting this option to "Auto" or "Always." However, if you set it to "None," your wireless router should be able to work fine, too.
Tx Power (11):	Set the wireless radio's output power. Unless you're using this wireless router in a really big space, you may not have to set the output power to 100%. This will enhance security (malicious/unknown users farther away will not be able to reach your wireless router).
WMM (12):	Wi-Fi® MultiMedia (WMM) will enhance the data transfer performance of multimedia contents when they're being transferred over a wireless network. If you don't know what it is/not sure if you need it, it's safe to set this option to "Enable;" however, the default value is "Disable."

After you finish these wireless settings, click on the "Apply" button. The following message will be displayed:

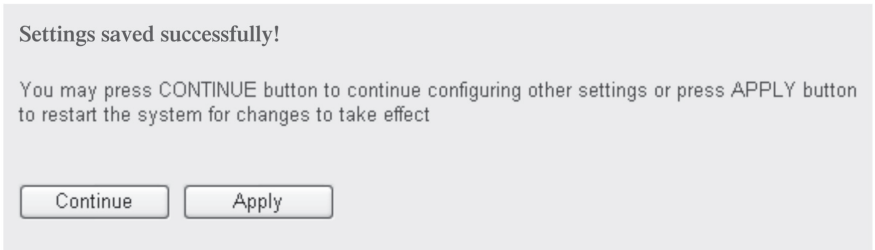

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 3-69. Settings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu to continue with router setup or click on the "Apply" button to reboot the router so the settings will take effect (wait for about 30 seconds while the router reboots).

3.7.3 Wireless Security

It's very important to set wireless security settings properly! If you don't, hackers and malicious users can reach your network and valuable data without your consent, compromising security.

To set wireless security settings, click on the "Wireless" menu on the left of the Web management interface, then click on "Security Settings." Follow these instructions to set wireless security settings:

Select an encryption method from the Encryption drop-down menu; there are four options: disable wireless security, WEP, WPA, and WPA radius.

Disable wireless security

When you select this mode, data encryption is disabled, and every wireless device nearby will be able to connect to your wireless router if no other security measure is enabled (such as MAC address access control—see Section 3.7.4, or disable ESSID broadcast). Only use this option when you really want to allow everyone to use your wireless router, and you don't care if someone reads the data you transfer over the network without your consent.

WEP—Wired Equivalent Privacy

When you select this mode, the wireless router will use WEP encryption, and the following setup menu will be displayed:

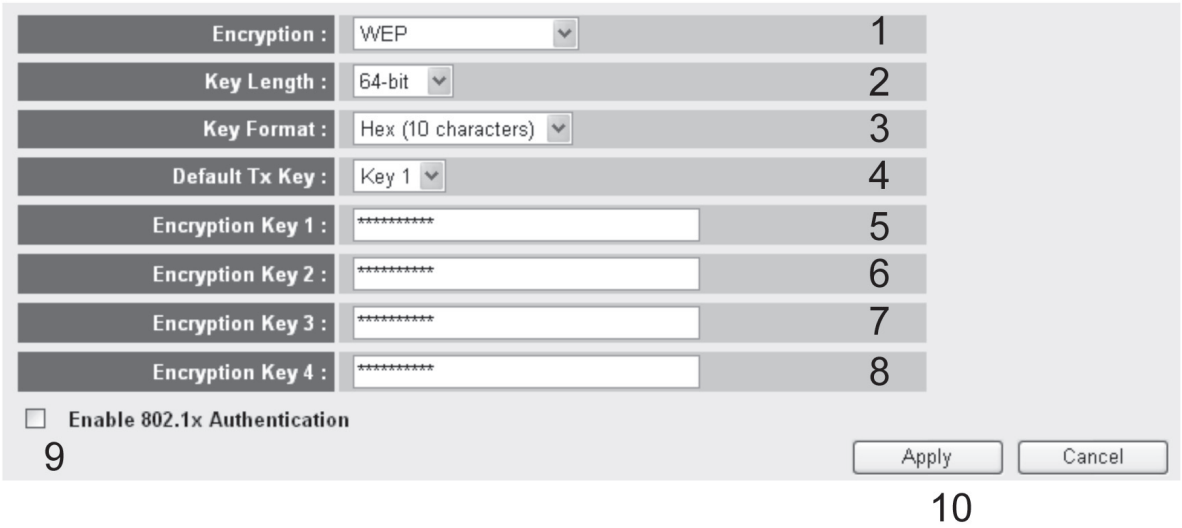


Figure 3-70. WEP setup menu.

Table 3-28. WEP setup menu options.

Item	Description
Key Length (2):	There are two WEP key lengths: 64-bit and 128-bit. Using 128-bit is safer than 64-bit but will reduce some data transfer performance.
Key Format (3):	There are two types of key formats: ASCII and Hex. When you select a key format, the number of key characters will be displayed. For example, if you select 64-bit as key length, and Hex as key format, you'll see that the message at the right of Key Format is Hex (10 characters), which means the WEP key length is 10 characters.

Table 3-28 (continued). WEP setup menu options.

Item	Description
Default Tx Key (4):	You can set up to four WEP keys, and you can decide which key is being used by default here. If you don't know which one you should use, select "Key 1."
Encryption Key 1 to 4 (5–8):	Input WEP key characters here. The number of characters must be the same as the number displayed in the Key Format field. You can use any alphanumerical characters (0-9, a-z, and A-Z) if you select ASCII key format. You can use characters 0-9, a-f, and A-F if you select Hex as key format. You must enter at least one encryption key here, and if you entered multiple WEP keys, they should not match each other.
Enable 802.1x Authentication (9):	IEEE 802.1x is an authentication protocol. Every user must use a valid account to log in to this wireless router before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates users by IEEE 802.1x, but it does not encrypt the data during communication. If there is a RADIUS server in your environment, enable this function. Check this box and another sub-menu will appear.

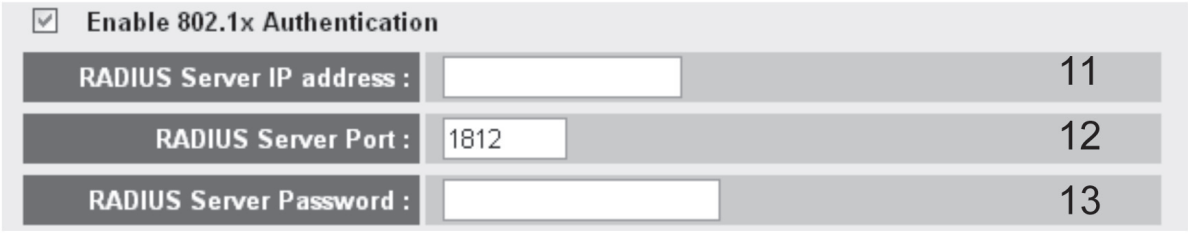


Figure 3-71. Enable 802.1x authentication screen.

Table 3-29. 802.1x authentication screen options.

Item	Description
RADIUS Server IP address (11):	Input the radius server's IP address here.
RADIUS Server Port (12):	Input the radius server's port number here.
RADIUS Server Password (13):	Input the radius server's password here.

TIPS: Some examples of the WEP key are shown below. Don't use these examples; use one of your own.

ASCII (5 characters): pilot phone 23561 2Hyux #AxmL

ASCII (13 characters): digitalFAMILY 82Jh26xHy3m&n

Hex (10 characters): 287d2aa732 1151dabc85

Hex (26 characters): 9284bcda8427c9e036f7abcd844

To improve the security level, don't use words that you can find in a dictionary or are to easy to remember (pilot and phone listed above are bad examples, they were just used to show you what a WEP key looks like). Wireless clients will remember your WEP key, so you only have to input the WEP key on a wireless client once. Use a complicated WEP key for maximum security.

After you finish the WEP setting, please click on the "Apply" button (10) and the following message will be displayed:

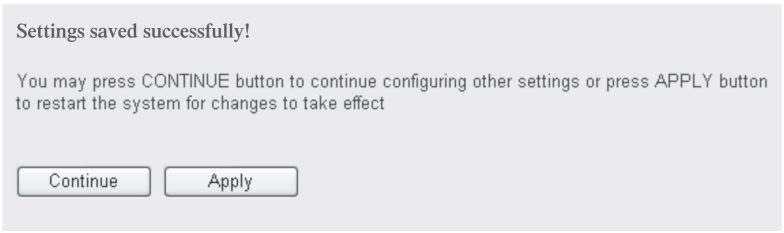

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 3-72. Settings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu to continue with other setup procedures. Click on the "Apply" button to reboot the router so the settings will take effect (please wait for about 30 seconds while the router reboots).

Wi-Fi Protected Access (WPA)

When you select this mode, the wireless router will use WPA encryption, and the following setup menu will be displayed:

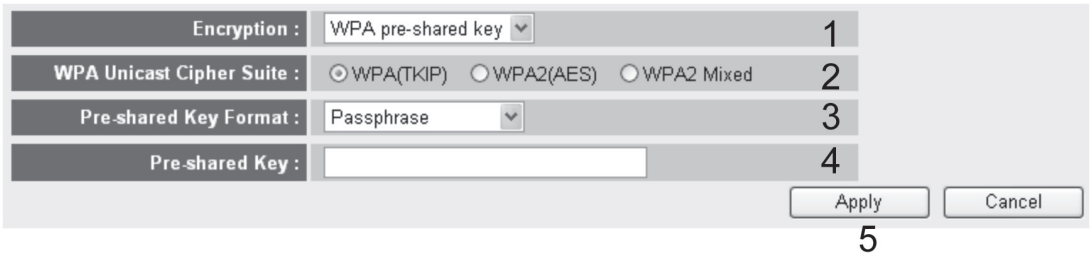


Figure 3-73. WPA setup screen.

Table 3-30. WPA options.

Item	Description
WPA Unicast Cipher Suite (2):	Select a type of WPA cipher suite. Available options are: WPA (TKIP), WPA2 (AES), and WPA2 Mixed. Select one of them, but make sure your wireless client supports the cipher you selected.
Pre-shared Key Format (3):	Select the type of pre-shared key format. You can select "Passphrase" (8 or more alphanumerical characters, up to 63), or "Hex" (64 characters of 0–9, and a–f).
Pre-shared Key (4):	Input the WPA passphrase here. Do not use a word that's found in the dictionary; this will compromise security.

After you finish the WPA Pre-shared key setting, please click on the "Apply" button (5) and the following message will be displayed:

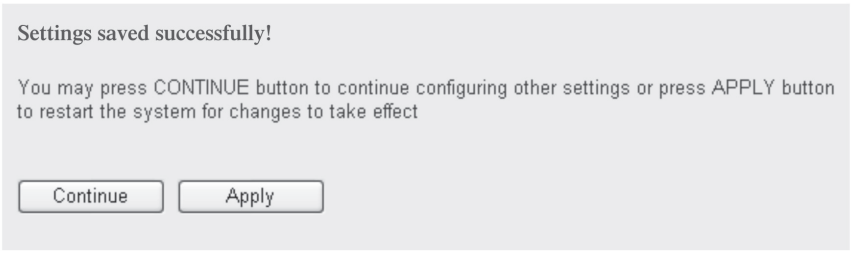

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 3-74. Settings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu to continue with other setup procedures. Click on the "Apply" button to reboot the router so the settings will take effect (please wait for about 30 seconds while the router reboots).

NOTE: Some wireless clients (especially those manufactured before the year 2003) only support WEP or WPA (TKIP) cipher. To use WPA and WPA2 encryption, you must upgrade the wireless client's software drivers.

WPA RADIUS

If you have a RADIUS server, this router can work with it and provide safer wireless authentication.

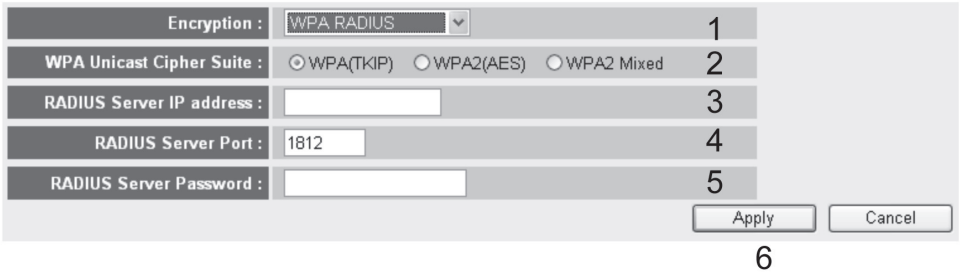


Figure 3-75. WPA RADIUS setup.

Table 3-31. WPA RADIUS options.

Item	Description
WPA Unicast Cipher Suite (2):	Select a WPA cipher suite. Available options are: WPA (TKIP), WPA2 (AES), and WPA2 Mixed. You can select one of them, but make sure your wireless client supports the cipher you selected.
RADIUS Server	Input the radius authentication server's IP address here.
RADIUS Server Port (4):	Input the radius authentication server's port number here. The default setting is 1812.
RADIUS Server Password (5):	Input your radius authentication server's password here.

After you finish with the settings, click on the "Apply" (6) button and the following message will be displayed:

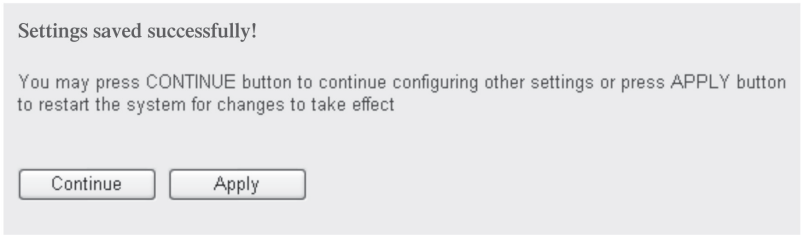

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 3-76. Settings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu to continue with other setup procedures or click on the "Apply" button to reboot the router so the settings will take effect (please wait for about 30 seconds while the router reboots).

3.7.4 Wireless Access Control

This function helps prevent unauthorized users from connecting to your wireless router; only wireless devices that have the MAC address you assign here can access your wireless router. Use this function with other security measures described in the previous section to create a safer wireless environment.

You can assign up to 20 MAC addresses using this function. Click on the "Wireless" menu on the left of the Web management interface, then click on "Access Control," and the following message will be displayed:

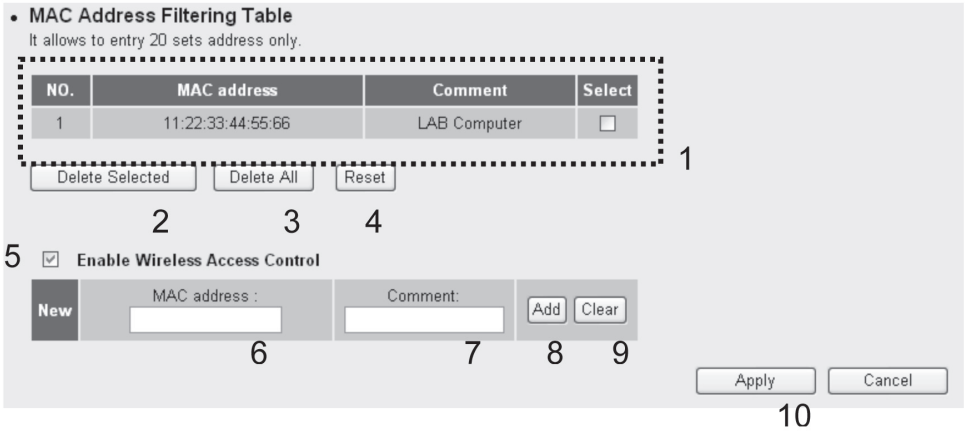


Figure 3-77. Wireless access control screen.

All allowed MAC addresses will be displayed in the MAC Address Filtering Table (1).

Table 3-32. Wireless access control screen options.

Item	Description
Delete Selected (2):	To delete a specific MAC address entry, check the select box for the MAC address you want to delete, then click on the "Delete Selected" button. (You can select more than one MAC address).
Delete All (3):	To delete all MAC addresses listed here, click on the "Delete All" button.
Reset (4):	Click on the "Reset" button to de-select all MAC addresses.
Enable Wireless Access Control (5):	To enforce MAC address filtering, check "Enable Wireless Access Control." When this item is unchecked, the wireless router will not enforce MAC address filtering for wireless clients.
MAC Address (6):	Input your wireless device's MAC address here; dash (-) or colon (:) are not required. (that is, If the MAC address label of your wireless device indicates 'aa-bb-cc-dd-ee-ff' or 'aa:bb:cc:dd:ee:ff', just input aabbccddeeff.
Comment (7):	Input any text here as the comment for this MAC address, such as "ROOM 2A Computer." Input up to 16 alphanumerical characters here. This is optional and you can leave it blank, however, we recommend that you use this field to write a comment for every MAC address as a memory aid.
Add (8):	Click on the "Add" button to add the MAC address and associated comment to the MAC address filtering table.
Clear (9):	Click on the "Clear" button to remove the value you input in the MAC address and comment field.

After you finish with the settings, please click on the "Apply" (10) button and the following message will be displayed:

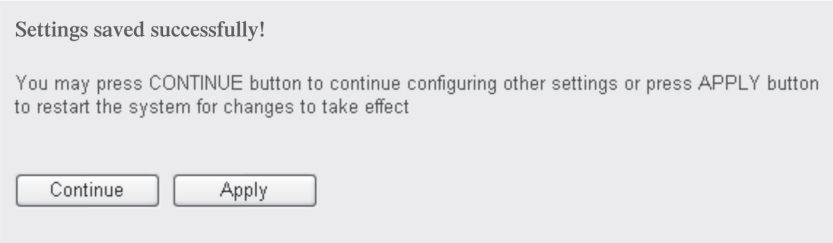

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 3-78. Settings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu to continue with other setup procedures. Click on the "Apply" button to reboot the router so the settings will take effect (wait for about 30 seconds while the router reboots).

To reset all settings in this page back to the previously saved values, click on the "Cancel" button.

3.7.5 Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) is the simplest way to build a connection between wireless network clients and this wireless router. You don't have to select an encryption mode and input a long encryption passphrase every time you need to setup a wireless client, just press a button on a wireless client and this wireless router, and the WPS will do the rest for you.

This wireless router supports two types of WPS: Push-Button Configuration (PBC) and PIN code. If you want to use PBC, you have to push a specific button on the wireless client to start WPS mode, and switch this wireless router to WPS mode, too. To do this, press the wireless router's "Reset/WPS" button, or click on the "Start PBC" button in the Web configuration interface. If you want to use PIN code, you have to know the wireless client's PIN code and switch it to WPS mode, then provide the PIN code of the wireless client you want to connect to this wireless router. Detailed instructions are listed on the next page:

Click on the wireless router's menu on the left of the Web management interface, then click "WPS," and the following message will be displayed:

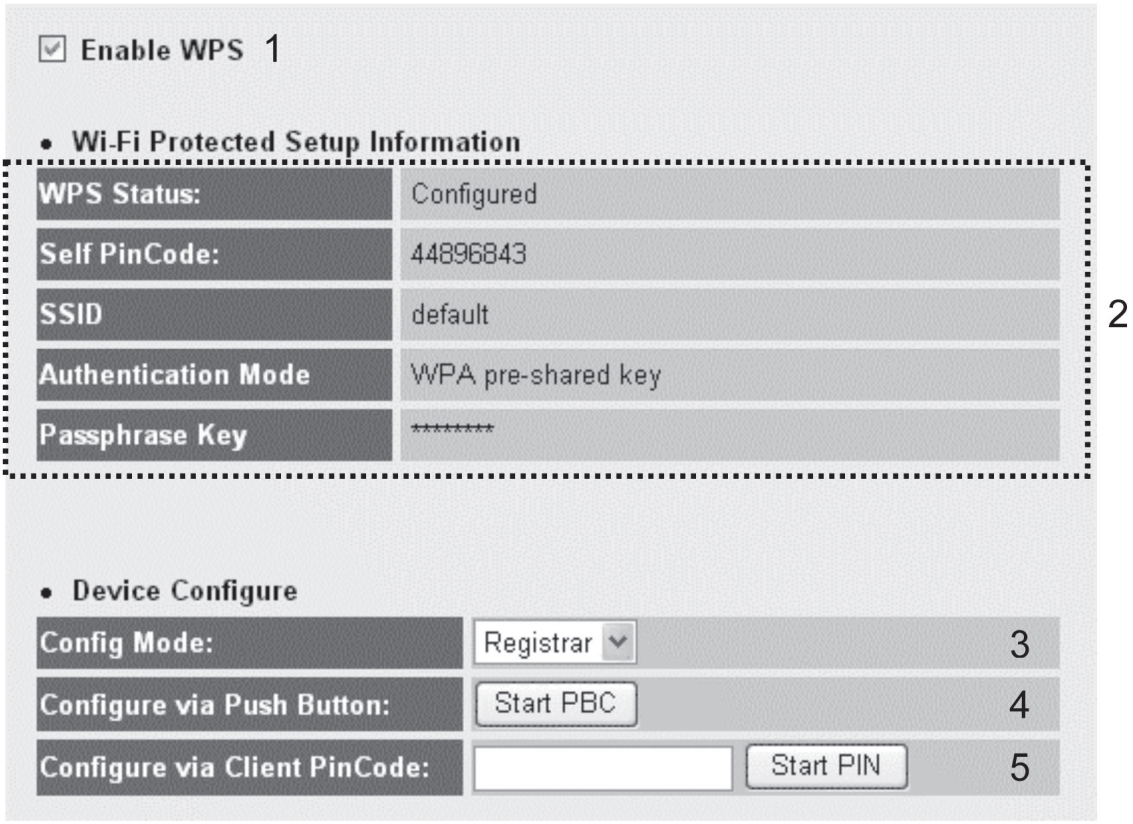


Figure 3-79. Enable WPS screen.

Table 3-33. Enable WPS screen options.

Item	Description
Enable WPS (1):	Check this box to enable the WPS function; uncheck it to disable WPS.
Wi-Fi Protected Setup Information (2):	WPS-related system information will be displayed here. WPS Status: If the router's wireless security (encryption) function is properly set, you'll see a "Configured" message here. If the wireless security function has not been set, you'll see "unConfigured." Self PIN code: This is the wireless router's WPS PIN code. Use this code when you need to create a wireless connection by WPS with other WPS-enabled wireless devices. SSID: The wireless router's SSID will be displayed here. Authentication Mode: The router's wireless security authentication mode will be displayed here. If you don't enable the wireless router's security function before WPS is activated, the router will auto set the security to "WPA (AES)" and generate a set of passphrase keys for WPS connection. Passphrase Key: The router's wireless security key will be displayed here.

Table 3-33 (continued). Enable WPS screen options.

Item	Description
Config Mode (3):	There are Registrar and Enrollee modes for the WPS connection. When "Registrar" is enabled, the wireless clients will follow the router's wireless settings for WPS connection. When "Enrolled" mode is enabled, the router will follow the wireless client's wireless settings for WPS connection.
Configure via Push Button (4):	Click "Start PBC" to start Push-Button style WPS setup procedure. This wireless router will wait for WPS requests from wireless clients for 2 minutes. The WLAN LED on the wireless router will be steady on for 2 minutes when this wireless router waits for an incoming WPS request.
Configure via client PinCode (5):	Input the wireless client's PIN code you want to connect and click on the "Start PIN" button. The WLAN LED on the wireless router will be steady on when this wireless router waits for incoming WPS requests.

3.7.6 Security Tips for Wireless Networks

Here are some quick tips to help you improve your wireless network's security level:

1. Never use simple words (like school, apple, and computer) as a WEP encryption or WPA passphrase.
2. Choose a complicated WEP key and WPA passphrase: it's much safer than simple and short ones. (For example, the passphrase should be a combination of numbers, letters, even symbols, and it should be long enough.) Remember that the wireless client can keep the key or passphrase for you, so you only have to input the complicated key or passphrase once. This will greatly improve security.
3. To hide the the router's ESSID, set the Broadcast ESSID option to "Disable." Your wireless router will not be found by other people nearby if they're just using their wireless client's AP scanning function. This will increase security.
4. Use the Access Control function described in Section 3.7.4, so people who are not on your list will not be able to connect to your network.

4. Advanced Functions

4.1 Quality of Service (QoS)

Quality of service provides an efficient way for computers on the network to share Internet bandwidth with a promised quality of Internet service. Without QoS, all computers and devices on the network will compete with each other to get internet bandwidth, and some applications that require guaranteed bandwidth (like video streaming and network telephony) would be affected, and video/audio transfer would also be affected.

With this function, you can limit the maximum bandwidth or give a guaranteed bandwidth for a specific computer.

4.1.1 Basic QoS Settings

Follow these instructions to set QoS parameters:

Click on the "QoS" menu on the left of the web management interface and the following message will be displayed:

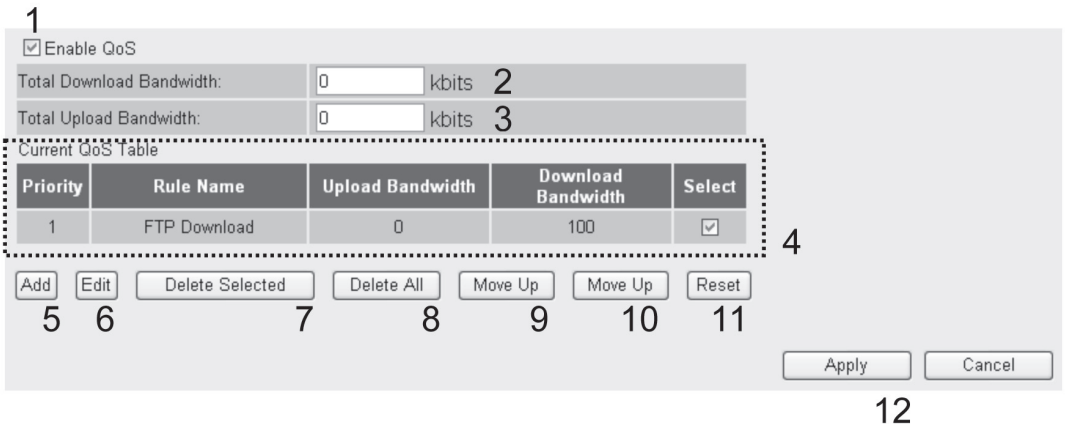


Figure 4-1. Enable QoS settings screen.

Table 4-1. Enable QoS options.

Item	Description
Enable QoS (1):	Check this box to enable QoS function, unselect this box if you don't want to enforce QoS bandwidth limitations.
Total Download Bandwidth (2):	You can set the limit of total download bandwidth in kbits. To disable the download bandwidth limitation, input "0" here.
Total Upload Bandwidth (3):	You can set the limit of total upload bandwidth in kbits. To disable the upload bandwidth limitation, input "0" here.
Current QoS Table (4):	All existing QoS rules will be displayed here.
Add (5):	Click on the "Add" button to add a new QoS rule (See Section 4.1.2, Add a New QoS rule.)
Edit (6):	If you want to modify the content of a specific rule, please check the select box of the rule you want to edit, then click on the "Edit" button. Only one rule should be selected a time! If you didn't select a rule before clicking on the "Edit" button, you'll be prompted to add a new rule.

Table 4-1 (continued). Enable QoS options.

Item	Description
Delete Selected (7):	Click on this button to delete selected rules. To select one or more rules to delete, check the select box for the rule(s) you want to delete. If the QoS table is empty, this button will be grayed out and can not be clicked.
Delete All (8):	Click on this button to delete all rules currently in the QoS table. If the QoS table is empty, this button will be grayed out and can not be clicked.
Move Up (9):	To increase the priority of the QoS rule you selected, click on this button.
Move Down (10):	To lower the priority of the QoS rule you selected, click on this button.
Reset (11):	To erase all values you just entered, click on the Reset button.

After you finish with the settings, click on the Apply (12) button and the following message will be displayed:

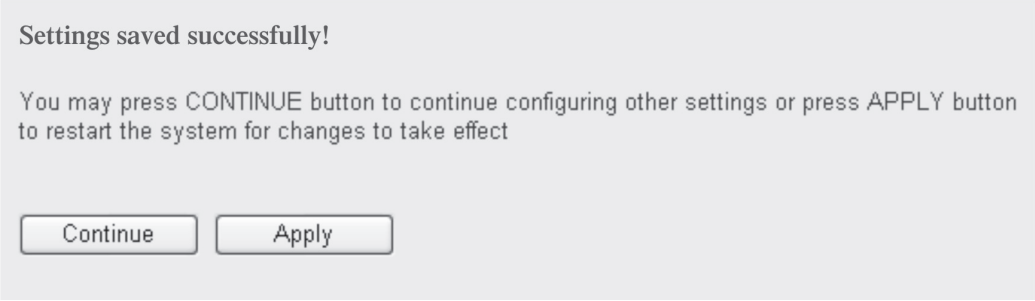

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 4-2. Settings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu to continue with other setup procedures. Click on the "Apply" button to reboot the router so the settings will take effect (please wait for about 30 seconds while the router reboots).

To reset all settings in this page back to the previously saved values, click on the "Cancel" button.

4.1.2 Add a New QoS Rule

After you click on the "Add" button in the QoS menu, the following message will appear:

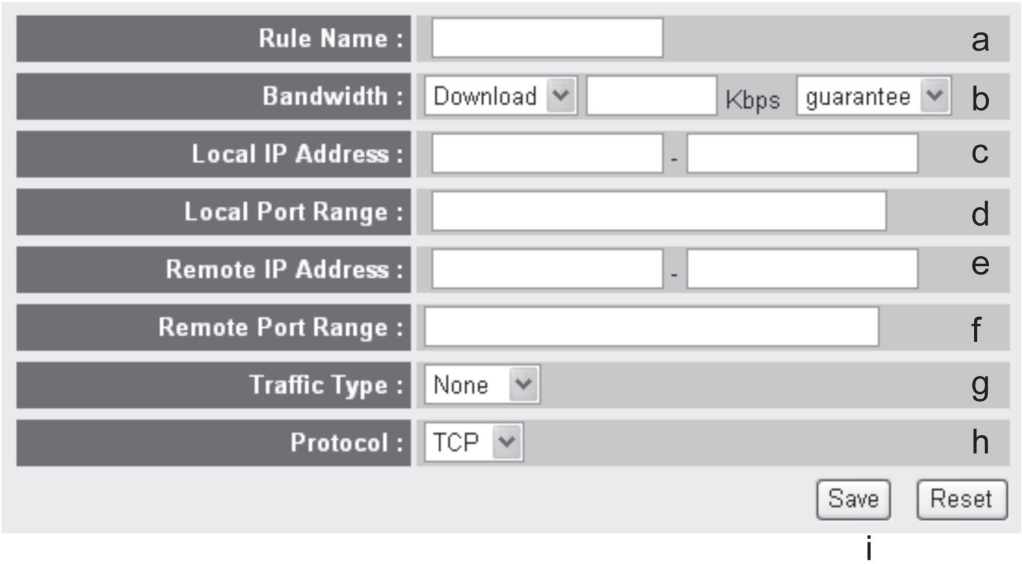


Figure 4-3. Add a new QoS rule.

Table 4-2. Add a new QoS rule options.

Item	Description
Rule Name (a):	Assign a name (up to 15 alphanumeric characters) to this QoS rule.
Bandwidth (b):	Set the bandwidth limitation of this QoS rule. Select the data direction of this rule (upload or download), and the speed of bandwidth limitation in kbps, then select the type of QoS: guarantee (guaranteed usable bandwidth for this rule) or max (set the maximum bandwidth for the application allowed by this rule).
Local IP Address (c):	Specify the local (source) IP address that will be affected by this rule. Input the starting IP address in the left field, and input the end IP address in the right field to define a range of IP addresses, or just input the IP address in the left field to define a single IP address.
Local Port Range (d):	Input the range of local (source) port numbers that will be affected by this rule. If you want to apply this rule on ports 80 to 90, input "80–90;" if you want to apply this rule on a single port, just input the port number, for example, "80."
Remote IP Address: (e):	Specify the remote (destination) IP address that will be affected by this rule. Input the starting IP address in the left field, and input the end IP address in the right field to define a range of IP addresses, or just input the IP address in the left field to define a single IP address.
Remote Port Range (f):	Input the range for the remote (destination) port numbers that will be affected by this rule. To apply this rule on port 80 to 90, input "80–90." To apply this rule on a single port, just input the port number, such as "80." If the remote (destination) IP address and/or port number is universal, just leave it blank.
Traffic Type (g):	Select the traffic type for this rule. Available options are None, SMTP, HTTP, POP3, and FTP. You can select a specific traffic type for this rule. To make this rule an IP address-based rule (apply the limitation on all traffic from/to the specified IP address/port number), select "None."

Table 4-2 (continued). Add a new QoS rule options.

Item	Description
Protocol (h):	Select the protocol type for this rule. Available options are TCP and UDP. If you don't know what protocol your application uses, try "TCP" first, and switch to "UDP" if this rule doesn't work.

After you finish with the settings, click on the "Save" button (i). You'll be brought back to the previous menu, and the rule you just set will appear in the current QoS table. If you did anything wrong, you'll get an error message when you click on the "Save" button. Correct your input by following the instructions given by the error message.

To erase all values you just entered, click on the "Reset" button.

4.2 Network Address Translation (NAT)

Network address translations enable sharing a single IP address for multiple computers. Without NAT, all computers must be assigned a valid Internet IP address to connect to the Internet. Since Internet service providers only provide a few IP addresses to every user, use NAT technology to share a single Internet IP address with multiple computers on the local network.

Follow these instructions to set NAT parameters:

4.2.1 Basic NAT Settings (Enable or Disable NAT Function)

Click on the "NAT" menu on the left of the Web management interface, and the following message will be displayed:

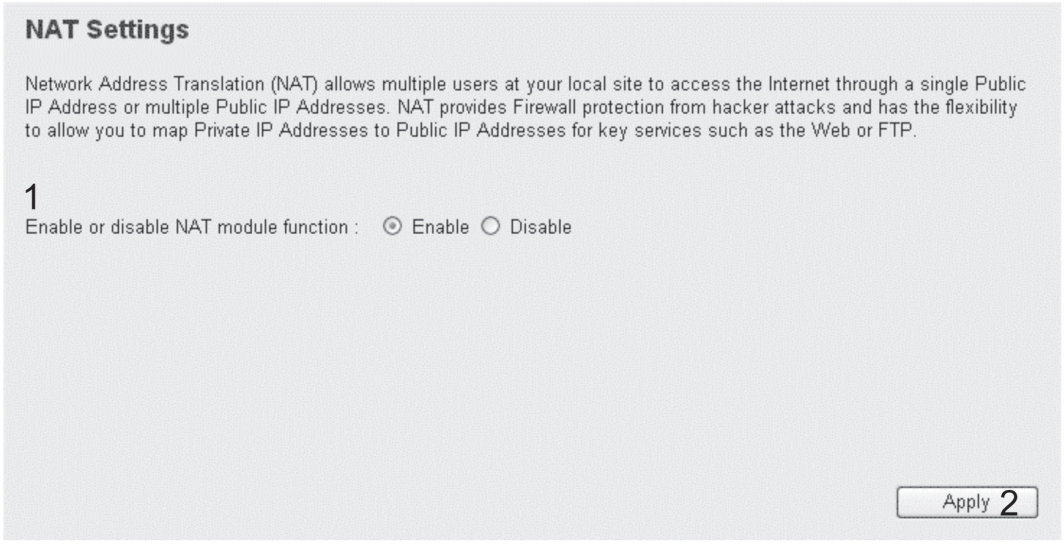

NAT Settings
Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as the Web or FTP.
1
Enable or disable NAT module function :
Enable
Disable
Apply
2

Figure 4-4. NAT settings screen.

To enable NAT function, select "Enable" for Enable NAT module function (1); to disable, select "Disable."

After you make the selection, click on the "Apply" button (2) and the following message will be displayed:

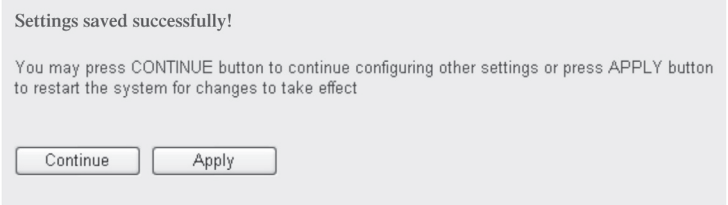

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 4-5. Settings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu to continue with other setup procedures. Click on the "Apply" button to reboot the router so the settings will take effect (please wait for about 30 seconds while the router reboots).

4.2.2 Port Forwarding

This function allows you to redirect a single port or consecutive ports of the Internet IP address to the same port of the IP address on the local network. The port number(s) of Internet IP address and private IP address (the IP address on the local network) must be the same. If the port number for Internet IP address and private IP address is different, use the Virtual Server function, described in Section 4.2.3.

Click on the "NAT" menu on the left of the Web management interface, then click on "Port Forwarding," and the following message will be displayed:

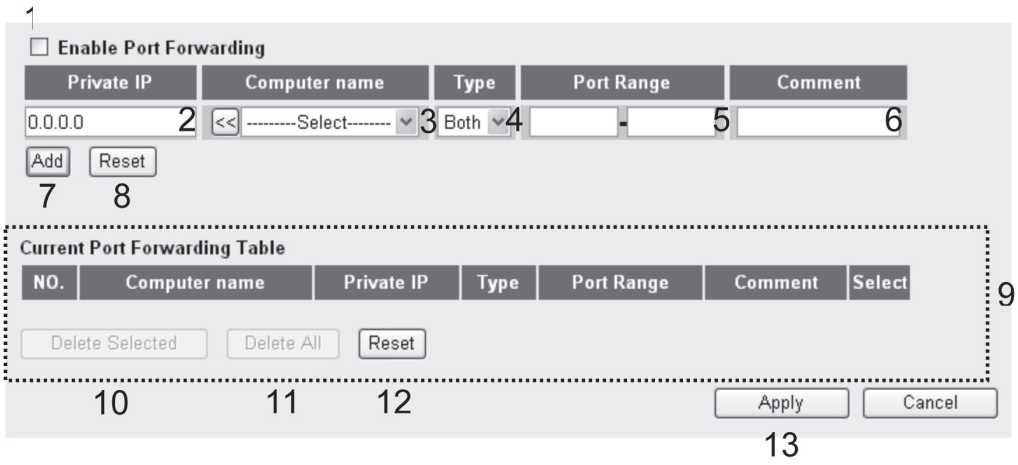


Figure 4-6. Enable port forwarding screen.

Table 4-3. Enable port forwarding screen options.

Item	Description
Enable Port Forwarding (1):	Check this box to enable port mapping; uncheck this box to disable port mapping.
Private IP (2):	Input the IP address of the computer on the local network that provides Internet service.
Computer Name (3):	Pull down the menu and all the computers connected to the router will be listed here. Select the computer name without checking the computer's IP address.
Type (4):	Select the connection type, TCP or UDP. If you're not sure, select "Both."
Port Range (5):	Input the starting port number in the left field, and input the ending port number in the right field. If you only want to redirect a single port number, just fill in the port number in the left field.
Comment (6):	Input any text (up to 16 alphanumeric characters) to describe this mapping.
Add (7):	Add the mapping to the port forwarding table.
Reset (8):	Remove all inputted values.
Port Forwarding Table (9):	All existing port forwarding mappings will be displayed here.

Table 4-3 (continued). Enable port forwarding options.

Item	Description
Delete Selected (10):	Select a port forwarding mapping by clicking on the mapping's "Select" box, then click on the "Delete Selected" button to remove the mapping. If there's no existing mapping, this button will be grayed out.
Delete All (11):	Delete all mappings from the virtual server table.
Reset (12):	De-select all mappings.

After you finish with the settings, click on the "Apply" (13) button and the following message will be displayed:

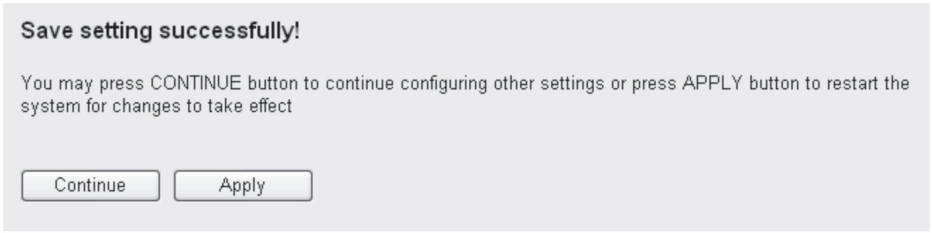

Save setting successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 4-7. Settings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu or to continue with other setup procedures. Click on the "Apply" button to reboot the router so the settings will take effect (please wait for about 30 seconds while the router reboots).

To reset all settings in this page back to the previously saved values, click on the "Cancel" button.

4.2.3 Virtual Server

This function allows you to redirect a port of an Internet IP address (on a WAN port) to a specified port of an IP address on a local network, so you can set up an Internet service on the computer on local network without exposing it directly to the Internet. You can also build many sets of port redirection to provide many different Internet services on different local computers via a single Internet IP address.

Click on the "NAT" menu on the left of the Web management interface, then click on "Virtual Server," and the following message will be displayed:

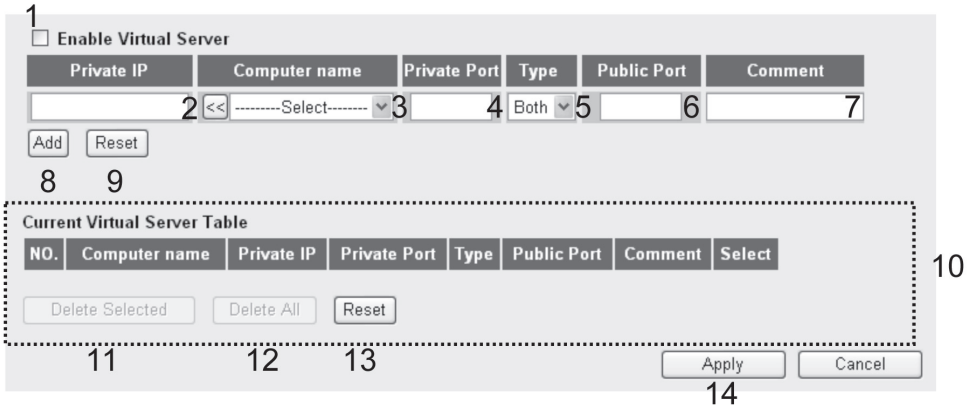


Figure 4-8. Enable virtual server screen.

Table 4-4. Enable virtual server options.

Item	Description
Enable Virtual Server (1):	Check this box to enable virtual server; uncheck this box to disable virtual server.
Private IP (2):	Input the IP address for the computer that provides Internet service.
Computer Name (3):	Pull down the menu, and all the computers connected to the router will be listed here. Select the computer name without checking the computer's IP address.
Private Port (4):	Input the port number of the IP address that provides Internet service.
Type (5):	Select the connection type, TCP or UDP. If you're not sure, select "Both."
Public Port (6):	Select the port number for the Internet IP address that will be redirected to the local IP address' port number defined above.
Comment (7):	Input any text (up to 16 alphanumeric characters) to describe this mapping.
Add (8):	Add the mapping to the virtual server table.
Reset (9):	Remove all inputted values.
Virtual Server Table (10):	All existing virtual server mappings will be displayed here.
Delete Selected (11):	Select a virtual server mapping by clicking on the "Select" box of the mapping, then click on the "Delete Selected" button to remove the mapping. If there's no existing mapping, this button will be grayed out.
Delete All (12):	Delete all mappings from the virtual server table.
Reset (13):	De-select all mappings.

After you finish with the settings, click on the "Apply" (14) button and the following message will be displayed:

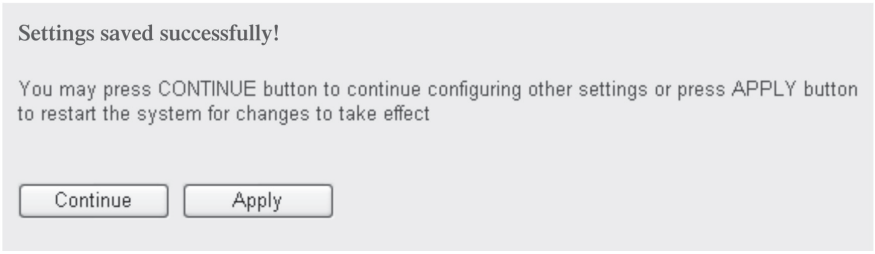

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 4-9. Settings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu or to continue with other setup procedures. Click on the "Apply" button to reboot the router so the settings will take effect (please wait for about 30 seconds while the router reboots).

If you want to reset the settings in this page back to the previously saved values, click on the "Cancel" button.

4.2.4 Port Mapping for Special Applications

Some applications require more than one connection a time; these applications won't work with simple NAT rules. To make these applications work, you can use the "Port Mapping" function.

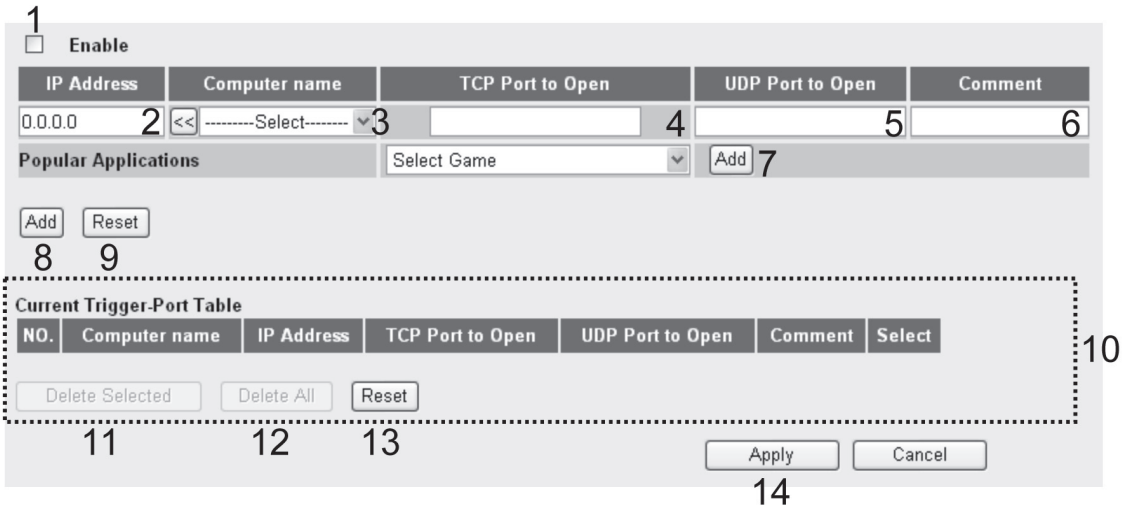


Figure 4-10. Port mapping screen.

Table 4-5. Port mapping options.

Item	Description
Enable (1):	Check this box to enable special applications and uncheck this box to disable the virtual server.
IP Address (2):	Input the IP address of the computer for which you want to open the ports.
Computer Name (3):	Pull down the menu, and all the computers connected to the router will be listed here. Select the computer name without checking the computer's IP address.
TCP Port to Open (4):	This is the outgoing (Outbound) range of TCP port numbers for this particular application.
UDP Port to Open (5):	This is the outgoing (Outbound) range of UDP port numbers for this particular application.
Comment (6):	The description of this setting.
Popular Applications (7):	This section lists the more popular applications that require multiple connections. Select an application from the "Popular Applications" selection and click on the "Add" button to save the settings to the Current Trigger-Port Table.
Add (8):	Add the settings to the Current Trigger-Port Table.
Reset (9):	Click on "Reset" to clear all the above settings. Then select the settings you want next.
Current Trigger-Port (10):	All the settings for the special applications will be listed here. If you want to remove some Special Application settings from the Current Trigger-Port Table, select them from the table and then click on the "Delete Selected" button. If you want remove all Special Application settings from the table, just click on the "Delete All" button. Click on the "Reset" button to clear your current selections.
Delete Selected (11):	Select a special application by clicking on the "Select" box of the mapping, then click on the "Delete Selected" button to remove the setting. If there's no setting here, this button will be grayed out.

Table 4-5 (continued). Port mapping options.

Item	Description
Delete All (12):	Delete all settings from the trigger port table.
Reset (13):	Unselect all settings.

NOTE: Only one LAN client can use a particular special application at a time.

After you finish with the settings, click on the "Apply" (14) button and the following message will be displayed:

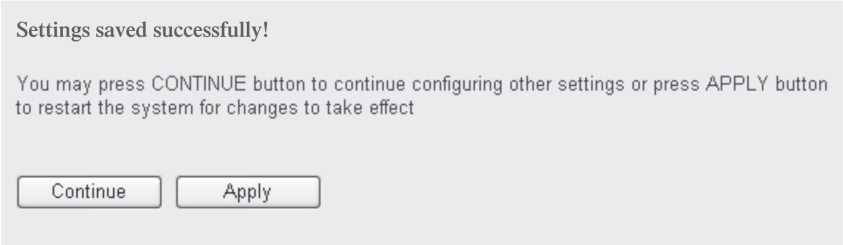

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 4-11. Savings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu or to continue with other setup procedures. Click on the "Apply" button to reboot the router so the settings will take effect (please wait for about 30 seconds while the router reboots).

To reset all settings in this page back to the previously saved values, click on the "Cancel" button.

4.2.5 UPnP Setting

This function enables network auto-configuration for peer-to-peer communications. It enables network devices to communicate with other devices directly, and learn information about other devices. Many network device and applications rely on the UPnP function.

Click on the NAT menu on the left of the Web management interface, then click "UPnP," and the following message will be displayed:

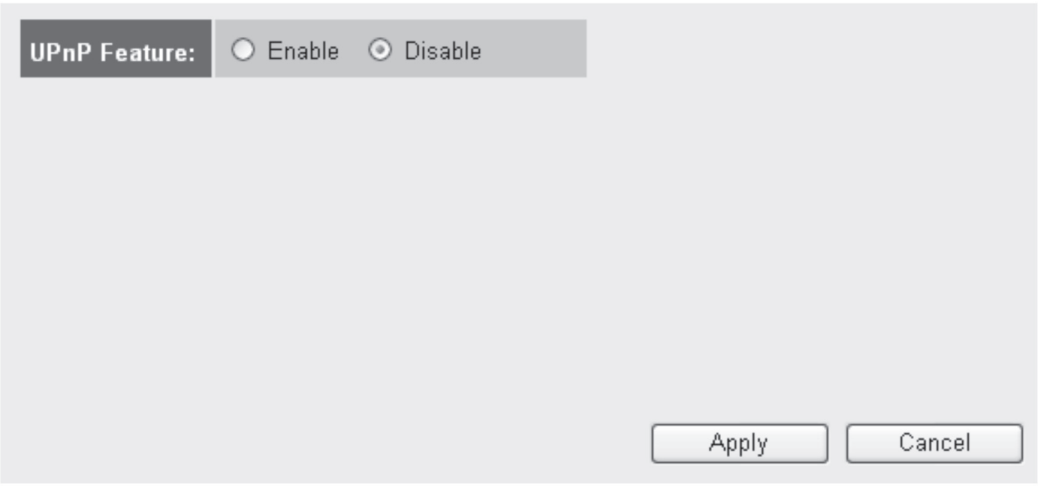


Figure 4-12. UPnP screen.

There is only one function in this page. Select "Enable" or "Disable" to enable or disable the UPnP function, then click on the "Apply" button, and the following message will be displayed:

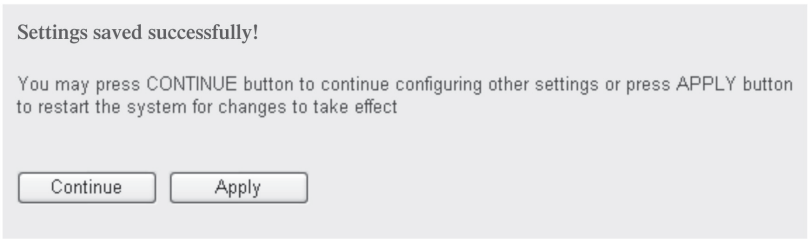

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 4-13. Settings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu or to continue with other setup procedures. Click on the "Apply" button to reboot the router so the settings will take effect (please wait for about 30 seconds while the router reboots).

To reset all settings in this page back to the previously saved values, click on the "Cancel" button.

4.2.6 ALG Settings

Application Layer Gateway (ALG) is a special function of this router. It includes many preset routing rules for numerous applications that require special support. With these rules, those applications that require special support will be able to work with NAT architecture.

Click on the NAT menu on the left of the Web management interface, then click on "ALG Settings," and the following message will be displayed:

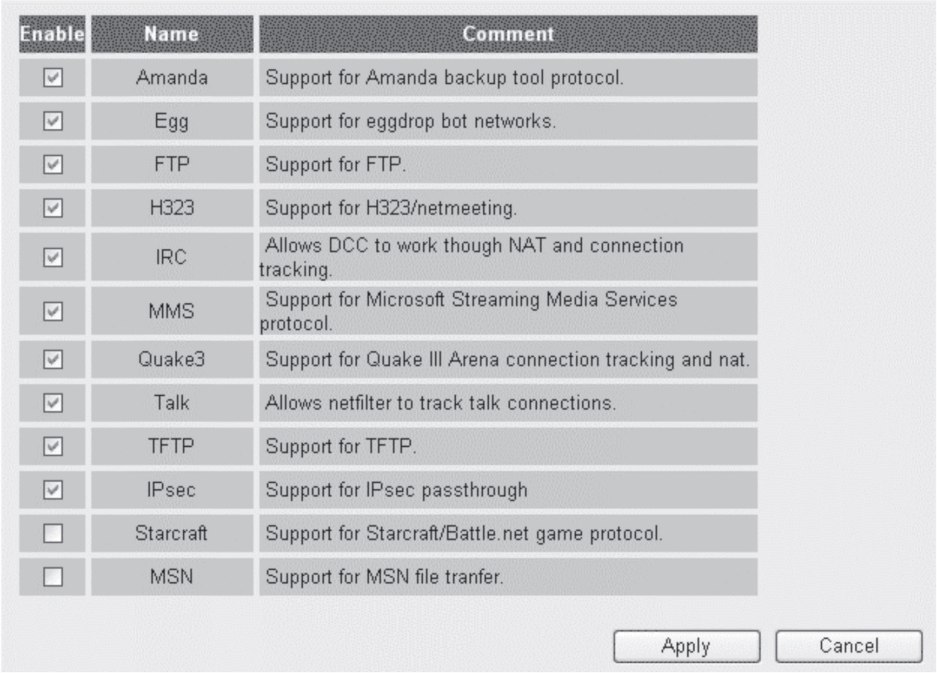


Figure 4-14. ALG settings screen.

There are many applications listed here. Check the boxes for the special support for applications you need, then click on the "Apply" button. The following message will be displayed:

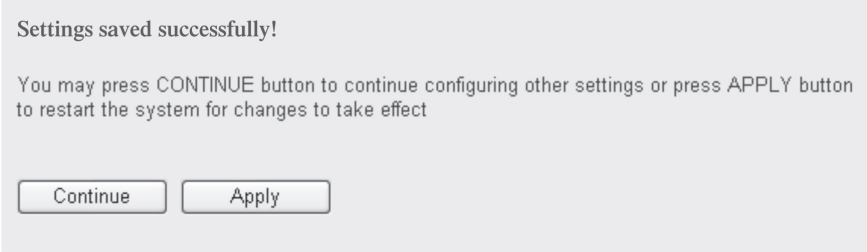

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 4-15. Settings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu or to continue with other setup procedures. Click on the "Apply" button to reboot the router so the settings will take effect (please wait for about 30 seconds while the router reboots).

To reset all settings in this page back to the previously saved values, click on the "Cancel" button.

4.3 Firewall

Except for NAT, this router also provides a firewall function to block malicious intruders from accessing your computers on the local network. These functions include inbound attack prevention. They also block outbound traffic, for example, they block URLs that have pre-defined keywords.

Follow these instructions to enable or disable the firewall function:

Click on the "Firewall" menu on the left of the Web management interface, and the following message will be displayed:

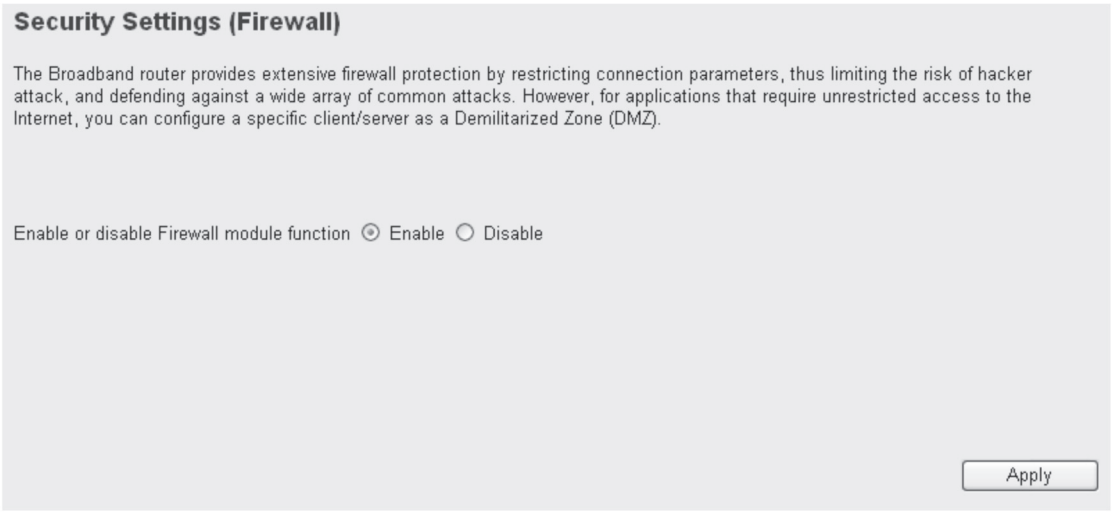

Security Settings (Firewall)
The Broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attack, and defending against a wide array of common attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).
Enable or disable Firewall module function Enable Disable
Apply

Figure 4-16. Firewall screen.

Select "Enable" or "Disable" to enable or disable the router's firewall function. Click on the "Apply" button, and the following message will be displayed:

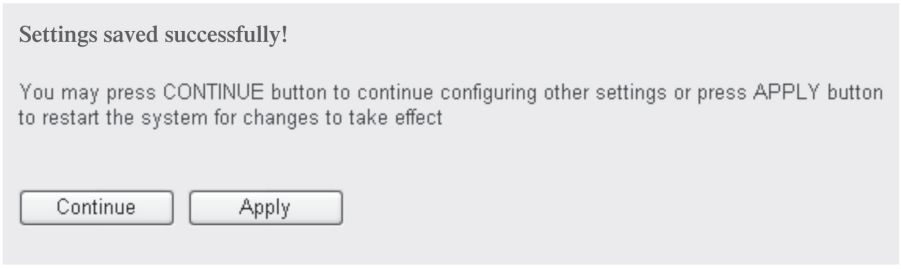

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 4-17. Settings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu or to continue with other setup procedures. Click on the "Apply" button to reboot the router so the settings will take effect (please wait for about 30 seconds while the router reboots).

4.3.1 Access Control

This function allows or denies computers with a specific MAC address from connecting to the network; it can also allow or deny computers with a specific IP address, protocol, or port.

Click on the "Firewall" menu on the left of the web management interface, then click on "Access Control." The following message will be displayed:

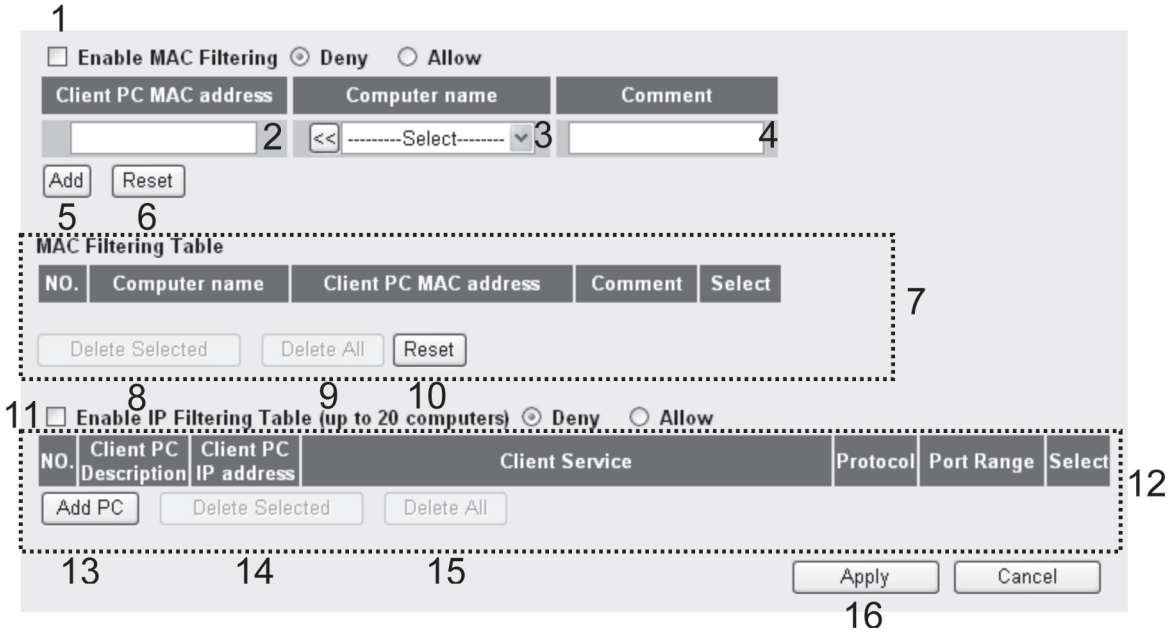


Figure 4-18. MAC filtering screen.

Table 4-6. MAC filtering options.

Item	Description
Enable MAC Filtering (1):	Check this box to enable MAC address based filtering, and select "Deny" or "Allow" to decide the behavior of the MAC filtering table. If you select "Deny," all MAC addresses listed in filtering table will be denied from connecting to the network; if you select "Allow," only MAC addresses listed in filtering table will be able to connect to the network, rejecting all other MAC addresses.
Client PC MAC address (2):	Input the MAC address for the computer or network device here. A dash (-) or colon (:) is not required (that is, if the MAC address label of your wireless device indicates 'aa-bb-cc-dd-ee-ff' or 'aa:bb:cc:dd:ee:ff', just input 'aabbccddeeff').
Computer Name (3):	Pull down the menu and all the computers connected to the router will be listed here. Select the computer name without checking the computer's IP address.
Comment (4):	Input any text (up to 16 alphanumeric characters) here as the comment of this MAC address, for example, "ROOM 2A Computer." This is optional and you can leave it blank; however, we recommend using this field to write a comment for every MAC addresses as a memory aid.
Add (5):	Click on the "Add" button to add the MAC address and associated comment to the MAC address filtering table.
Reset (6):	Remove all inputted values.
MAC Filtering: Table (7)	All existing MAC addresses in the filtering table will be listed here.
Delete Selected (8):	To delete a specific MAC address entry, check the select box for the MAC address you want to delete, then click on the "Delete Selected "button. (You can select more than one MAC address).
Delete All (9):	To delete all MAC addresses listed here, click on the "Delete All" button.
Reset (10):	Click on the "Reset" button to de-select all MAC addresses.
Enable IP Filtering Table (11):	Check this box to enable IP address based filtering. Select "Deny" or "Allow" to decide the behavior of the IP filtering table. If you select deny, all IP addresses listed in the filtering table will be denied from connecting to the network; if you select allow, only IP addresses listed in the filtering table will be able to connect to the network, rejecting all other network devices.
IP Filtering Table (12):	All existing IP addresses in the filtering table will be listed here.
Add PC (13):	Click on this button to add a new IP address to the IP filtering table. You can add up to 20 IP addresses.
Delete Selected (14):	To delete a specific IP address entry, check the select box of the IP address you want to delete, then click on the "Delete Selected" button. (You can select more than one IP address).
Delete All (15):	To delete all IP addresses listed here, click on the "Delete All" button.

After you finish with the settings, click on the "Apply" (16) button, and the following message will be displayed:

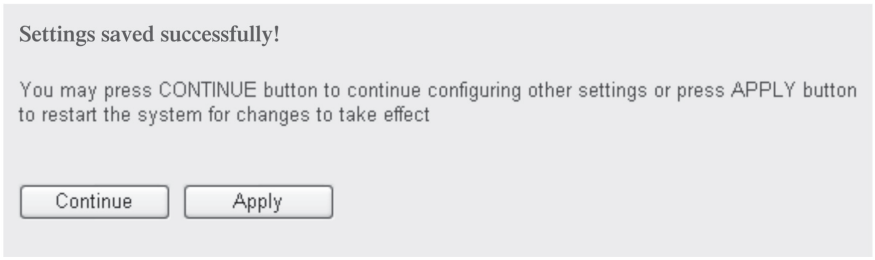

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 4-19. Settings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu or to continue with other setup procedures. Click on the "Apply" button to reboot the router so the settings will take effect (please wait for about 30 seconds while the router reboots).

To reset all settings in this page back to the previously saved values, click on the "Cancel" button.

Add PC

After you click on the "Add PC" button, the following message will be displayed:

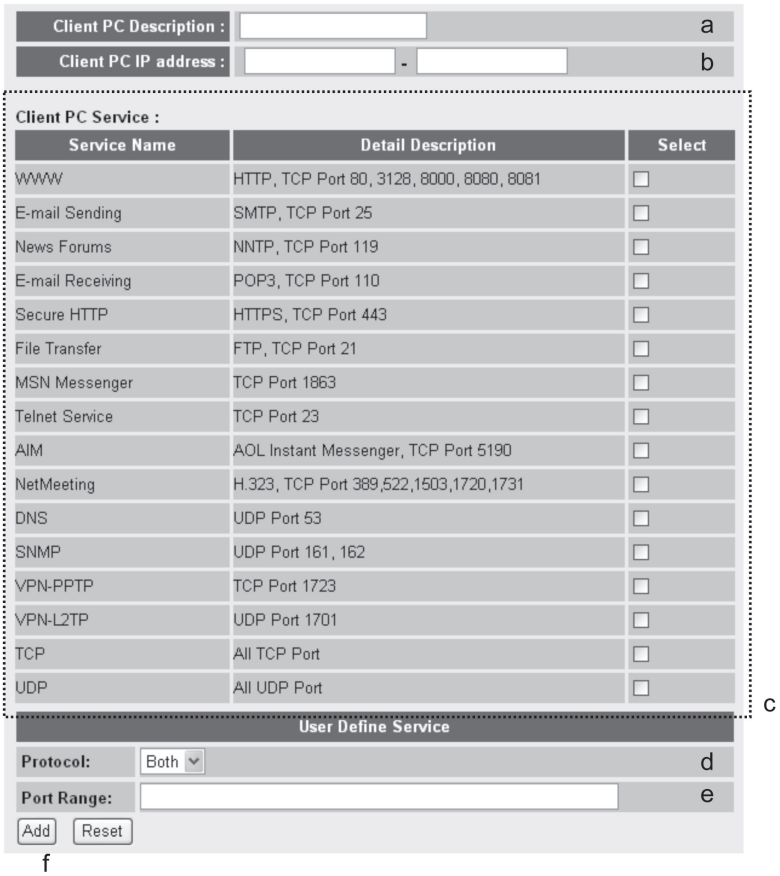


Figure 4-20. Add PC screen.

Table 4-7. Add PC options.

Item	Description
Client PC Description (a):	Input any text (up to 16 alphanumeric characters) to describe this IP address.
Client PC IP address (b):	Input the starting IP address in the left field, and input the end IP address in the right field to define a range of IP addresses, or just input the IP address in the left field to define a single IP address.
Client PC Service (c):	Check all services you want to allow or deny this IP address to use. You can check multiple services.
Protocol (d):	If the service you need is not listed above, create a new service on your own. Select TCP or UDP; if you're not sure, select "Both."
Port Range (e):	Input the port range of the new service here. If you want to specify ports 80 to 90, input "80–90." If you want to apply this rule on a single port, just input the port number, for example, "80."
Add (f):	When you finish with all settings, click on the "Add" button to save the settings. You'll be brought back to the previous menu, and the rule you just set will appear in the current IP filtering table.

If you want to remove all settings in this page, click on the "Reset" button.

4.3.2 URL Blocking

To prevent computers in the local network from accessing certain Web sites (such as pornography, violence, or anything you want to block), use this function to stop computers in your local network from accessing the site you defined here.

This function is useful for parents and company managers.

Follow these instructions to set URL blocking parameters:

Click on the "Firewall" menu on the left of the Web management interface, then click on "URL Blocking." The following message will be displayed:

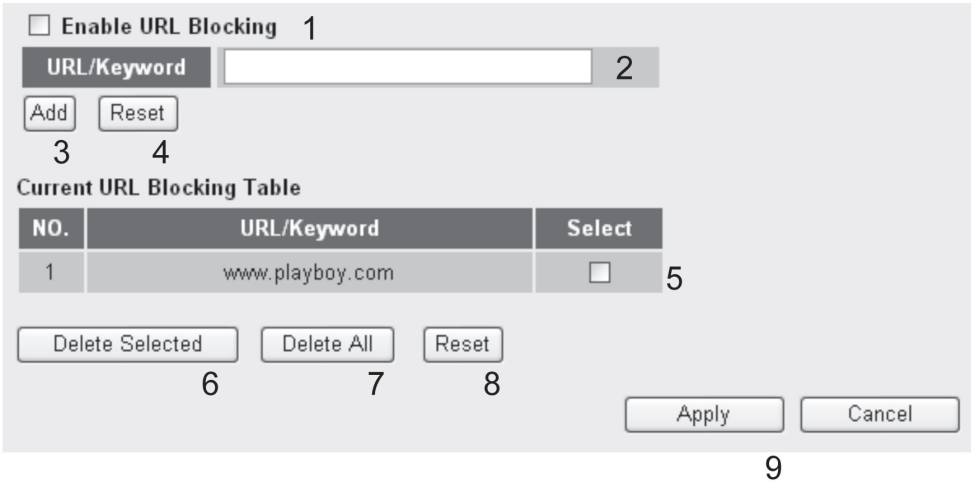


Figure 4-21. URL blocking screen.

Table 4-8. URL blocking options.

Item	Description
Enable URL Blocking (1):	Check this box to enforce URL Blocking, uncheck it to disable URL Blocking.
URL/Keyword (2):	Input the URL (host name or IP address of the Web site, like http://www.blocked-site.com or http://11.22.33.44), or the keyword that's in the URL (like pornography, cartoon, stock, etc.).
Add (3):	Click on the "Add" button to add the URL/keyword to the URL/Keyword filtering table.
Reset (4):	Click on the "Reset" button to remove the value you inputted in the URL/Keyword field.
Current URL Blocking Table (5):	All existing URL/Keywords in the filtering table will be listed here.
Delete Selected (6):	To delete a specific URL/Keyword entry, check the select box for the MAC address you want to delete, then click on the "Delete Selected" button. (You can select more than one MAC address).
Delete All (7):	To delete all URL/Keyword listed here, click on the "Delete All" button.
Reset (8):	You can also click on the "Reset" button to unselect all URL/Keywords.

After you finish with the settings, please click on the "Apply" (9) button, and the following message will be displayed:

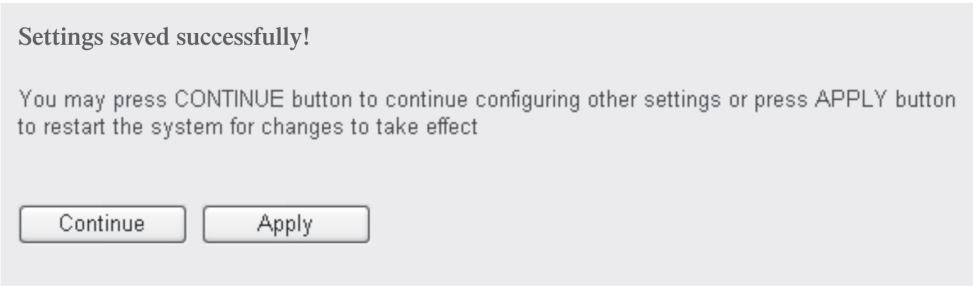

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 4-22. Settings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu or to continue with other setup procedures. Click on the "Apply" button to reboot the router so the settings will take effect (please wait for about 30 seconds while the router reboots).

If you want to reset all settings in this page back to the previously saved values, click on the "Cancel" button.

4.3.3 DoS Attack Prevention

Denial of Service (DoS) is a common attack measure. It transmits a great amount of data or requests to your Internet IP address and server. The Internet connection will become very slow, and the server may stop responding because it can't handle too much traffic.

This router has a built-in DoS attack prevention mechanism; when you activate it, the router will stop the DoS attack for you.

Follow these instructions to set DoS prevention parameters:

Click on the "Firewall" menu on the left of the Web management interface, then click on "DoS." The following message will be displayed:

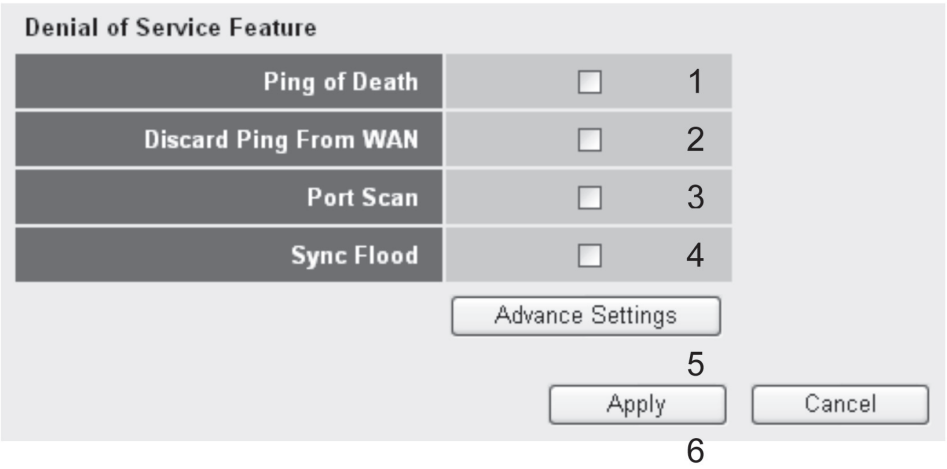


Figure 4-23. DoS screen.

Table 4-9. DoS options.

Item	Description
Ping of Death (1):	Ping of Death is a special packet, and it will cause certain computers to stop responding. Check this box and the router will filter out this kind of packet.
Discard Ping From WAN (2):	Ping is a common and useful tool to know the connection status of a specified remote network device, but some malicious intruder might try to fill your network bandwidth with a lot of ping request data packets, to slow down your Internet connection or make it unusable. Check this box and the router will ignore all inbound ping requests; but when you activate this function, you will not be able to ping your own router from the Internet, either.
Port Scan (3):	Some malicious intruder might try to use a port scanner to know how many ports of your Internet IP address are open, and they can collect a lot of valuable information by doing so. Check this box and the router will block all traffic that's trying to scan your Internet IP address.
Sync Flood (4):	This is another kind of attack, which uses a lot of fake connection requests to consume the memory of your server to try to make your server become unusable. Check this box and the router will filter out this kind of traffic.
Advanced Settings (5):	Click this button and you can set the advanced settings for the DoS prevention method listed above.

After you finish with the settings, click on the "Apply" (6) button and the following message will be displayed:

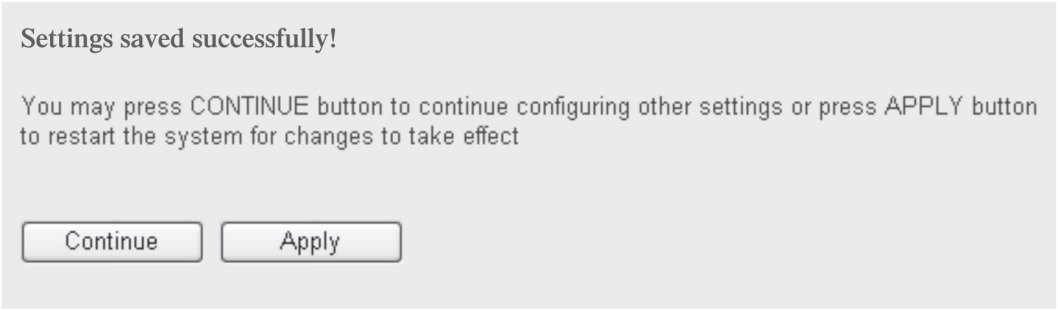

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 4-24. Settings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu or to continue with other setup procedures. Click on the "Apply" button to reboot the router so the settings will take effect (please wait for about 30 seconds while the router reboots).

To reset all settings in this page back to the previously saved values, click on the "Cancel" button.

DoS—Advanced Settings

When you click on the "Advanced" button in the DoS menu, the following message will be displayed:

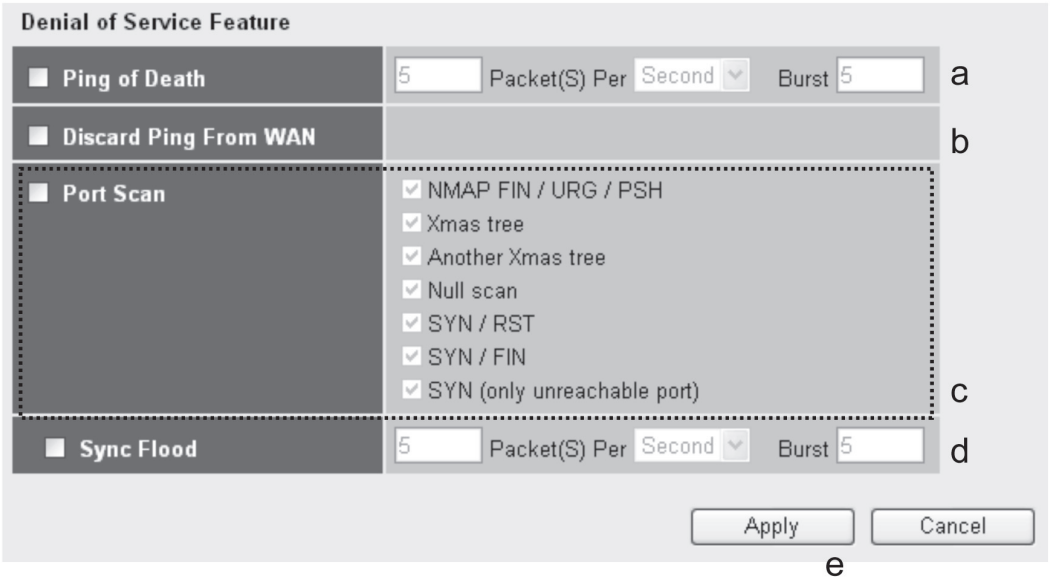


Figure 4-25. DoS advanced settings screen.

Table 4-10. DoS advanced settings options.

Item	Description
Ping of Death (a):	Set the threshold of when this DoS prevention mechanism will be activated. Check the box for Ping of Death and input the frequency for the threshold (how many packets per second, minute, or hour). You can also input the Burst value, which means when this number for the Ping of Death packet is received in a very short time, this DoS prevention mechanism will be activated.

Table 4-10 (continued). DoS advanced settings options.

Item	Description
Discard Ping from WAN (b):	Check the box to activate this DoS prevention mechanism.
Port Scan (c):	Many port scan methods are listed here. Check one or more DoS attack methods you want to prevent.
Sync Flood (d):	Like Ping of Death, you can set the threshold for when this DoS prevention mechanism will be activated.

After you finish with the settings, click on the "Apply" (e) button and the following message will be displayed:

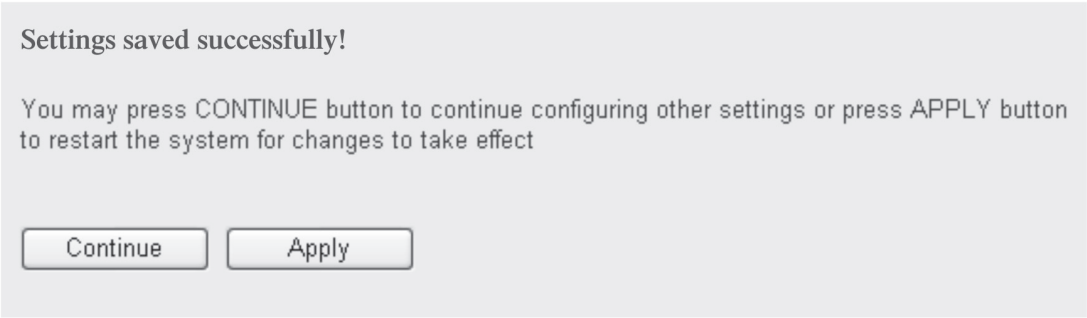

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 4-26. Settings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu or to continue with other setup procedures. Click on the "Apply" button to reboot the router so the settings will take effect (please wait for about 30 seconds while the router reboots).

To reset all settings in this page back to the previously saved values, click on the "Cancel" button.

4.3.4 Demilitarized Zone (DMZ)

Demilitarized Zone (DMZ) refers to a special area in your local network. This area resides on the local network, and all computers in this area use private IP addresses, too. These private IP addresses are mapped to a certain Internet IP address, so other people on the Internet can fully access those computers in DMZ.

Follow these instructions to set DMZ parameters:

Click on the "Firewall" menu on the left of the Web management interface, then click "DMZ." The following message will be displayed:

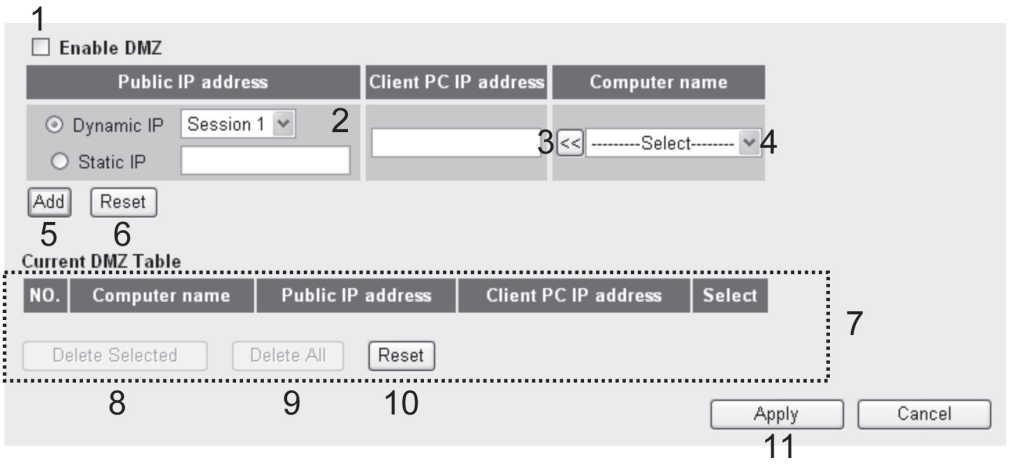


Figure 4-27. DMZ screen.

Table 4-11. DMZ options.

Item	Description
Enable DMZ (1):	Check this box to enable the DMZ function; uncheck this box to disable the DMZ function.
Public IP address (2):	Select "Dynamic IP" or "Static IP" here. If you select "Dynamic IP," you have to select an Internet connection session from a drop-down menu. If you select "Static IP," input the IP address that you want to map to a specific private IP address.
Client PC IP address (3):	Input the private IP address that the Internet IP address will be mapped to.
Computer Name (4):	Pull down the menu and all the computers connected to the router will be listed here. Select the computer name without checking the computer's IP address.
Add (5):	Click on the "Add" button to add the public IP address and associated private IP address to the DMZ table.
Reset (6):	Click on the "Clear" button to remove the value you inputted in the Public IP address and Client PC IP address fields.
Current DMZ table (7):	All existing public IP address and private IP address mapping will be displayed here.
Delete Selected (8):	To delete a specific DMZ entry, check the select box of the DMZ entry you want to delete, then click on the "Delete Selected" button. (You can select more than one DMZ entry.)
Delete All (9):	To delete all DMZ entries listed here, click on the "Delete All" button.
Reset (10):	Click on the "Reset" button to de-select all DMZ entries.

After you finish with the settings, click on the "Apply" (11) button and the following message will be displayed:

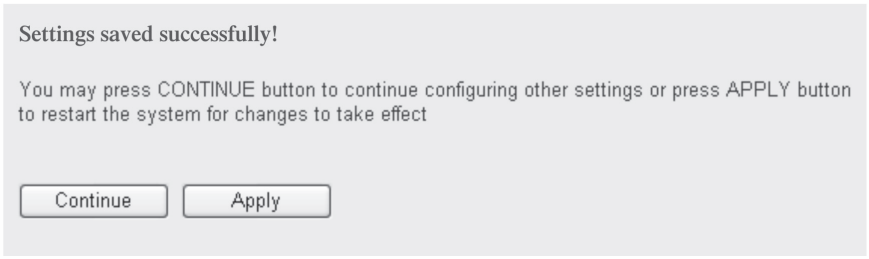

Settings saved successfully!
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
Continue
Apply

Figure 4-28. Settings saved successfully screen.

Click on the "Continue" button to go back to the previous setup menu or to continue with other setup procedures. Click on the "Apply" button to reboot the router so the settings will take effect (please wait for about 30 seconds while the router reboots).

To reset all settings in this page back to the previously saved values, click on the "Cancel" button.

4.4 System Status

The functions described here will provide you with system-related information. To enter the system status menu, either click on the Status link located at the upper-right corner of the Web management interface or click on the "Status" button in the main menu.

4.4.1 System Information and Firmware Version

Use this function to display the router's system information and firmware version.

Click on the Status link located at the upper-right corner of the Web management interface. The following message will be displayed.

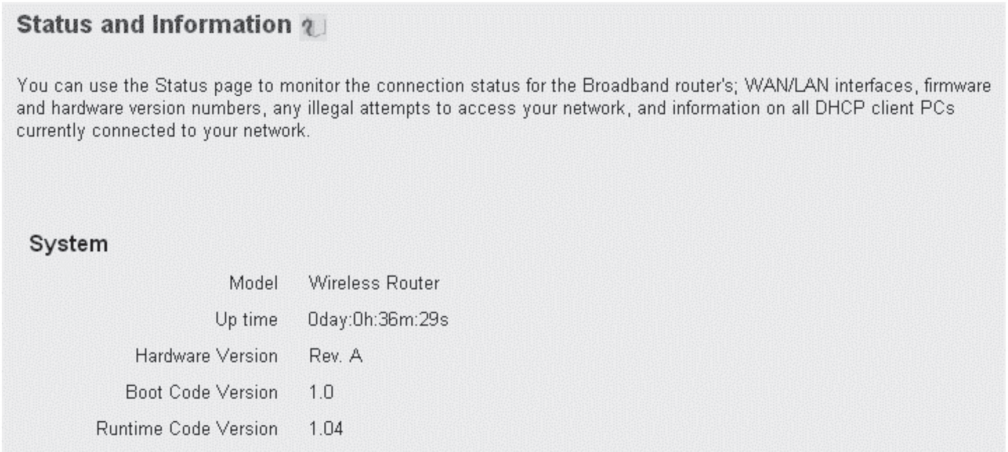

Status and Information
You can use the Status page to monitor the connection status for the Broadband router's; WAN/LAN interfaces, firmware and hardware version numbers, any illegal attempts to access your network, and information on all DHCP client PCs currently connected to your network.
System
Model Wireless Router
Up time 0day:0h:36m:29s
Hardware Version Rev. A
Boot Code Version 1.0
Runtime Code Version 1.04

Figure 4-29. Status and information screen.

NOTE: The information displayed here may vary.

4.4.2 Internet Connection Status

Use this function to display the current Internet connection's status.

Click on the Internet Connection menu on the left of the Web management interface. The following message will be displayed:

Attain IP Protocol :	Fixed IP connect
IP Address :	192.168.1.10
Subnet Mask :	255.255.255.0
Default Gateway :	192.168.1.254
MAC Address :	00:0E:2E:44:6B:02
Primary DNS :	192.168.0.2
Secondary DNS :	0.0.0.0

Figure 4-30. Internet connection status screen.

This information will vary depending on the connection status.

4.4.3 Device Status

Use this function to display the router's status.

Click on the "Device Status" menu on the left of the Web management interface, and the following message will be displayed:

Wireless Configuration	
Mode	AP
ESSID	default
Channel Number	1
Security	WEP
LAN Configuration	
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
DHCP Server	Disable
MAC Address	00:0e:2e:44:6b:01

Figure 4-31. Device status screen.

This information will vary depending on the device status.

4.4.4 System Log

All important system events are logged. Use this function to check the router's event log.

Click on the "System Log" menu on the left of the Web management interface, and the following message will be displayed:

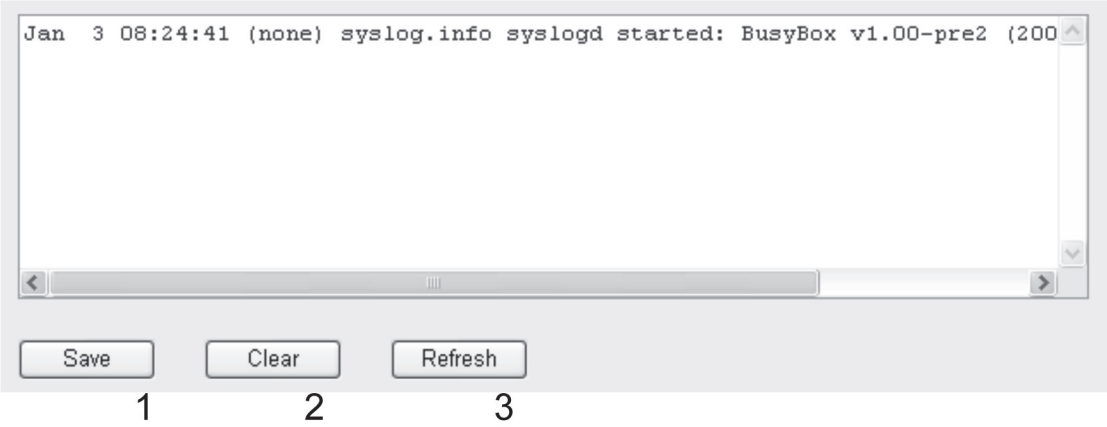


Figure 4-32. Sample system log.

The system events will be displayed in this page.

Table 4-12. System events options.

Item	Description
Save (1):	Save the current event log to a text file.
Clear (2):	Delete all event logs displayed here.
Refresh (3):	Refresh the event log display.

4.4.5 Security Log

All information about network and system security is kept here, and you can use this function to check the router's security event log.

Click on the "Security Log" menu on the left of the Web management interface, and the following message will be displayed:

Figure 4-33. Security log screen.

The system events will be displayed in this page.

Table 4-13. Security log options.

Item	Description
Save (1):	Save the current event log to a text file.
Clear (2):	Delete all event logs displayed here.
Refresh (3):	Refresh the event log display.

4.4.6 Active DHCP Client List

If you're using the router's DHCP server function, you can use the Active DHCP Client List function to check all active DHCP leases issued by this router.

Click on the "Active DHCP client" menu on the left of the Web management interface, and the following message will be displayed:

Figure 4-34. Active DHCP client list screen.

All information about active DHCP leases issued by this router will be displayed here. Click on the "Refresh" button to display the latest information.

4.4.7 Statistics

Use this function to check the router's wireless, LAN, and WAN interface status.

Click on the "Statistics" menu on the left of the Web management interface, and the following message will be displayed:

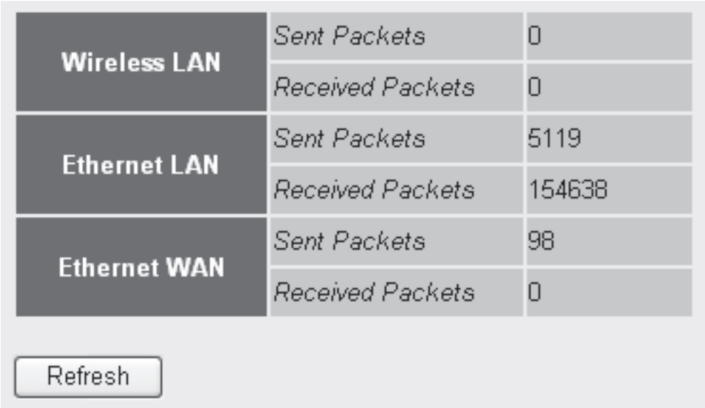


Figure 4-35. Statistics screen.

Click on the "Refresh" button to display the latest information.

4.5 Configuration Backup and Restore

You can back up all configurations of this router to a file, so you can make several copies of router configuration for security.

To back up or restore router configuration, follow these instructions:

Click on "Tool" located at the upper-right corner of the Web management interface, then click on "Configuration Tools" on the left of the Web management interface, and the following message will be displayed:

Figure 4-36. Backup and restore screen.

Table 4-14. Backup and restore options.

Item	Description
Backup Settings (1):	Press the "Save..." button, and you'll be prompted to download the configuration as a file. The default filename is config.bin. You can save it as another filename for different versions and keep it in a safe place.
Restore Settings (2):	Press the "Browse…" button to pick a previously saved configuration file from your computer, and then click on the "Upload" button to transfer the configuration file to the router. After the configuration is uploaded, the router's configuration will be replaced by the file you just uploaded.
Restore to Factory Default (3):	Click on this button to remove all settings you made, and restore the router's configuration back to factory default settings.

4.6 Firmware Upgrade

To upgrade firmware, please follow these instructions:

Click on "Tool" located at the upper-right corner of the Web management interface, then click on "Firmware Upgrade" on the left of the Web management interface. The following message will be displayed:

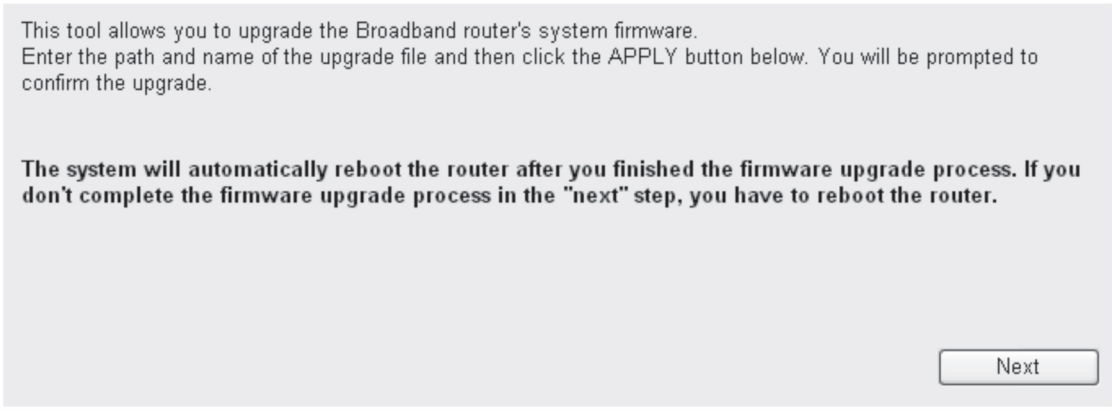

This tool allows you to upgrade the Broadband router's system firmware.
Enter the path and name of the upgrade file and then click the APPLY button below. You will be prompted to confirm the upgrade.
The system will automatically reboot the router after you finished the firmware upgrade process. If you don't complete the firmware upgrade process in the "next" step, you have to reboot the router.
Next

Figure 4-37. Firmware upgrade screen 1.

Click on "Next" and the following message will be displayed:

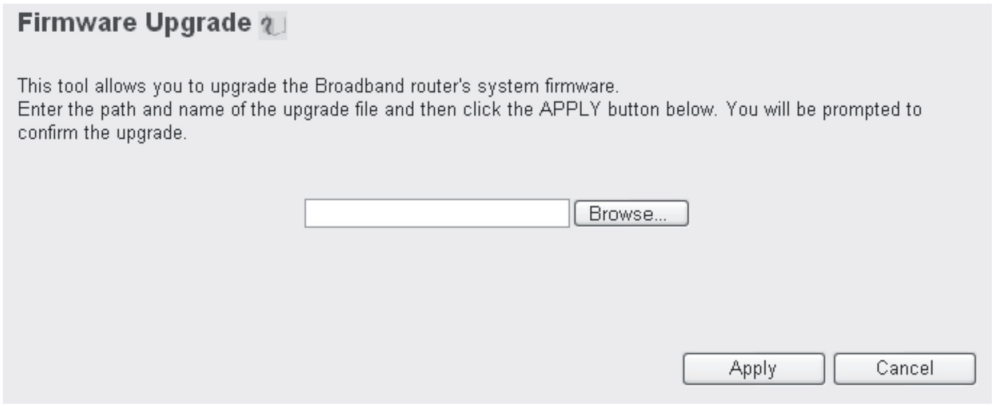

Firmware Upgrade
This tool allows you to upgrade the Broadband router's system firmware.
Enter the path and name of the upgrade file and then click the APPLY button below. You will be prompted to confirm the upgrade.
Browse...
Apply
Cancel

Figure 4-38. Firmware upgrade screen 2.

Click on the "Browse" button first and you'll be prompted to provide the firmware upgrade file's filename. Contact Tech Support at 724-746-5500.

4.7 System Reset

If the network performance is bad, or if the router's behavior is strange, you can perform a router reset to solve the problem.

Click on "Tool" located at the upper-right corner of the Web management interface, then click on the "Reset" button on the left of the web management interface. The following message will be displayed:

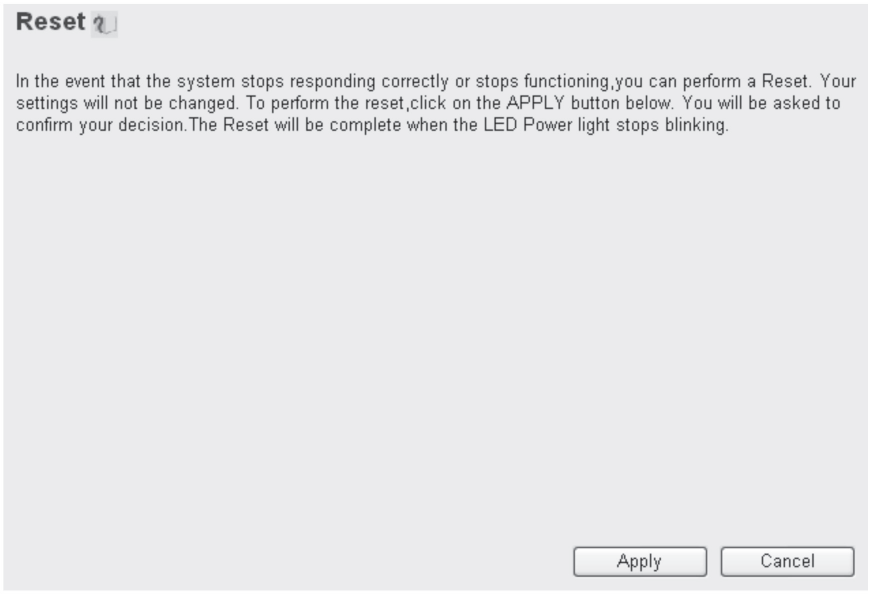

Reset
In the event that the system stops responding correctly or stops functioning,you can perform a Reset. Your settings will not be changed. To perform the reset,click on the APPLY button below. You will be asked to confirm your decision.The Reset will be complete when the LED Power light stops blinking.
Apply
Cancel

Figure 4-39. Reset screen.

Click on the "Apply" button to reset your router. It will be available again after few minutes, so please be patient.

Appendix A: Troubleshooting

If the router is working improperly or stops responding, please read this troubleshooting section first. You can solve some problems yourself in a few minutes.

A.1 Problems/Solutions

Problem: The router is not responding when I want to access it using a Web browser.

Solution: a. Check the router's power cord and network cable connections. All cords and cables should be correctly and firmly connected to the router.

b. If all LEDs on this router are off, check the status of the A/C power adapter, and make sure it's correctly powered.

c. You must use the same IP address section that the router uses.

d. Are you using a MAC or an IP address filter? Try to connect the router using another computer and see if it works; if not, restore your router to factory default settings (press the Reset button for more than 10 seconds).

e. Set your computer to obtain an IP address automatically (DHCP), and see if your computer can get an IP address.

f. If you did a firmware upgrade and this happens, contact Black Box Technical Support at 724-746-5500.

g. If all the above solutions don't work, contact Black Box Technical Support at 724-746-5500.

Problem: I can't connect to the Internet.

Solution: a. Go to the Status -> Internet Connection menu, and check the Internet connection status.

b. If this only happens sporadically, it could just be the Internet running slowly.

c. If you connected a computer to Internet directly before, try to do that again, and check if you can connect to the Internet with your computer directly attached to the device provided by your Internet service provider.

d. Check the PPPoE/L2TP/PPTP user ID and password again.

e. Call your Internet service provider and check if there's something wrong with their service.

f. If you just can't connect to one or more Web sites, but you can still use other Internet services, check the URL/Keyword filter.

g. Try to reset the router and try again later.

h. Reset the device provided by your Internet service provider, too.

i. Try to use IP address instead of hostname. If you can use IP address to communicate with a remote server, but can't use hostname, check the DNS setting.

Problem: I can't locate my router via my wireless client.

Solution: a. Is Broadcast ESSID set to off?

b. Are both antennas properly secured?

c. Are you too far from your router? Try to get closer.

d. Remember that you must input ESSID on your wireless client manually if ESSID broadcast is disabled.

Problem: File download is very slow or breaks frequently.

Solution: a. Are you using the QoS function? Disable it and try again.

b. If this only happens sporadically, it could just be the Internet running slowly.

c. Reset the router.

d. Know what computers do on your local network. If someone's transferring big files, other people will think the Internet is really slow.

e. If this never happened before, call your Internet service provider to find out if there is something wrong with their network.

Problem: I can't log onto the Web management interface: the password is wrong.

Solution: a. Make sure you're connecting to the router's correct IP address.

b. The password is case sensitive. Make sure the Caps Lock light is not on.

c. If you forgot the password, do a hard reset.

Problem: Router is hot.

Solution: a. This is not a malfunction if you can keep your hand on the router's case.

b. If you smell something wrong or see smoke coming out from router or A/C power adapter, disconnect the router and A/C power adapter from utility power, and call Black Box Technical Support at 724-746-5500.

Problem: The date and time of all event logs are wrong.

Solution: Adjust the router's internal clock.

A.2 Calling Black Box

If you determine that your router is malfunctioning, do not attempt to alter or repair the unit. It contains no user-serviceable parts. Contact Black Box Technical Support at 724-746-5500.

Before you do, make a record of the history of the problem. We will be able to provide more efficient and accurate assistance if you have a complete description, including:

- the nature and duration of the problem.
- when the problem occurs.
- the components involved in the problem.
- any particular application that, when used, appears to create the problem or make it worse.

A.3 Shipping and Packaging

If you need to transport or ship your router:

- Package it carefully. We recommend that you use the original container.
- If you are returning the unit, make sure you include everything you received with it. Before you ship for return or repair, contact Black Box to get a Return Authorization (RA) number.

Appendix B: Glossary

Default Gateway (Router): Every non-router IP device needs to configure a default gateway's IP address. When the device sends out an IP packet and the destination is not on the same network, the device has to send the packet to its default gateway, which will then send it out towards the destination.

DHCP: Dynamic Host Configuration Protocol. This protocol automatically gives every computer on your home network an IP address.

DNS Server IP Address: DNS stands for Domain Name System, which allows Internet servers to have a domain name (such as www.Broadbandrouter.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of Internet servers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing Broadbandrouter.com into your Internet browser), the user is sent to the proper IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

DSL Modem: Digital Subscriber Line Modem. A DSL modem uses your existing phone lines to transmit data at high speeds.

Ethernet: A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10 or 100 million bits per second (Mbps).

Idle Timeout: Idle Timeout is designed so that after there is no traffic to the Internet for a preconfigured amount of time, the connection will automatically be disconnected.

IP Address and Network (Subnet) Mask: IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods, which identifies a unique Internet computer host in an IP network. Example: 192.168.2.1. It consists of two portions: the IP network address, and the host identifier.

The IP address is a 32-bit binary pattern, which can be represented as four cascaded decimal numbers separated by ".": aaa.aaa. aaa.aaa, where each "aaa" can be anything from 000 to 255, or as four cascaded binary numbers separated by ".": bbbbbbbb. bbbbbbbb.bbbbbbbb.bbbbbbbb, where each "b" can either be 0 or 1.

A network mask is also a 32-bit binary pattern, and consists of consecutive leading 1's followed by consecutive trailing 0's, such as 11111111.11111111.11111111.00000000. Therefore, sometimes a network mask can also be described simply as "x" number of leading 1's. When both are represented side by side in their binary forms, all bits in the IP address that correspond to 1's in the network mask become part of the IP network address, and the remaining bits correspond to the host ID. For example, if the IP address for a device is, in its binary form, 11011001.10110000.10010000.00000111, and if its network mask is, 11111111.11111111.1 1110000.00000000, the device's network address is 11011001.10110000.10010000.00000000, and its host ID is 00000000.000 00000.00000000.00000111. This is a convenient and efficient method for routers to route IP packets to their destination.

ISP Gateway Address: (see ISP for definition). The ISP Gateway Address is an IP address for the Internet router located at the ISP's office.

ISP: Internet Service Provider. An ISP is a business that provides connections to the Internet for individuals and other businesses or organizations.

LAN: Local Area Network. A LAN is a group of computers and devices connected in a relatively small area (such as an office or a house). Your home network is considered a LAN.

MAC Address: MAC stands for Media Access Control. A MAC address is the hardware address of a device connected to a network. The MAC address is a unique identifier for a device with an Ethernet interface. It is comprised of two parts: three bytes of data that correspond to the Manufacturer ID (unique for each manufacturer), plus three bytes that are often used as the product's serial number.

NAT: Network Address Translation. This process allows all the computers on your home network to use one IP address. Using the broadband router's NAT capability, you can access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

Port: Network Clients (LAN PC) uses port numbers to distinguish one network application/protocol over another. Below is a list of common applications and protocol/port numbers:

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

PPPoE: Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a secure data transmission method originally created for dialup connections; PPPoE is for Ethernet connections. PPPoE relies on two widely accepted standards, Ethernet and the Point-to-Point Protocol. It is a communications protocol for transmitting information over Ethernet between different manufacturers.

Protocol: A protocol is a set of rules for interaction agreed upon between multiple parties so that when they interface with each other based on such a protocol, the interpretation of their behavior is well defined and can be made objectively, without confusion or misunderstanding.

Router: A router is an intelligent network device that forwards packets between different networks based on network layer address information such as IP addresses.

Subnet Mask: A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers (for example, 255.255.255.0) configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must be assigned by InterNIC).

TCP/IP, UDP: Transmission Control Protocol/Internet Protocol (TCP/IP) and Unreliable Datagram Protocol (UDP). TCP/IP is the standard protocol for data transmission over the Internet. Both TCP and UDP are transport layer protocol. TCP performs proper error detection and error recovery, and thus is reliable. UDP on the other hand is not reliable. They both run on top of the IP (Internet Protocol), a network layer protocol.

WAN: Wide Area Network. A network that connects computers located in geographically separate areas (for example, different buildings, cities, countries). The Internet is a wide area network.

Web-based management Graphical User Interface (GUI): Many devices support a graphical user interface that is based on the Web browser. This means you can use the familiar Netscape® or Microsoft® Internet Explorer® to control/configure or monitor the device being managed.

Black Box Tech Support: FREE! Live. 24/7.

Great tech support is just 30 seconds away at 724-746-5500 or blackbox.com.

BLACK BOX®
NETWORK SERVICES

About Black Box

Black Box Network Services is your source for an extensive range of networking and infrastructure products. You'll find everything from cabinets and racks and power and surge protection products to media converters and Ethernet switches all supported by free, live 24/7 Tech support available in 30 seconds or less.

© Copyright 2013. All rights reserved.

WRT-300BGN-R2, version 2